

POWERS IN ORBITS OF RATIONAL FUNCTIONS: CASES OF AN ARITHMETIC DYNAMICAL MORDELL-LANG CONJECTURE

JORDAN CAHN, RAFFAEL JONES, JACOB SPEAR

ABSTRACT. We classify, for fixed $m \geq 2$, the rational functions $\phi(x)$ defined over a number field K that have a K -orbit containing infinitely many distinct m th powers. For $m \geq 5$ the only such maps are those of the form $cx^j(\psi(x))^m$, while for $m \leq 4$ additional maps occur, including certain Lattès maps and four families of rational functions whose special properties appear not to have been studied before. Thus, unusual arithmetic properties of a single orbit of a rational function imply strong conclusions about the global structure of the function. With additional analysis, we show that the index set $\{n \geq 0 : \phi^n(a) \in \lambda(\mathbb{P}^1(K))\}$ is a union of finitely many arithmetic progressions, where ϕ^n denotes the n th iterate of ϕ and $\lambda \in K(x)$ is any map with two totally ramified fixed points in $\mathbb{P}^1(K)$. This result is similar in flavor to the dynamical Mordell-Lang conjecture, and motivates a new conjecture on the intersection of an orbit with the value set of a morphism. A key ingredient in our proofs is a study of the genera of curves of the form $y^m = \phi^n(x)$. We find, for example, that these genera either grow exponentially with n or are bounded by 1 as n grows. We classify all ϕ for which these genera remain bounded, and present many examples; as part of this analysis we give a complete account of the post-critical behavior of Lattès maps. Another outcome of our method is a classification of every $\phi \in \mathbb{C}(x)$ with an iterate that is an m th power in $\mathbb{C}(x)$.

1. INTRODUCTION

Let K be a field and $\phi \in K(x)$ a rational function of degree $d \geq 2$ defined over K . We denote by $\phi^n(x)$ the n th iterate of ϕ , which we emphasize is distinct from the n th power $\phi(x)^n$ of $\phi(x)$. A fundamental object in dynamics is the orbit

$$O_\phi(a) := \{\phi^n(a) : n \geq 0\}$$

of $a \in \mathbb{P}^1(K)$ under the map ϕ . In particular, a primary goal is to classify the orbits of a given map ϕ in terms of salient features of K , such as a metric or arithmetic structure. A related goal, which has attracted a large body of work, is to understand the collection of maps that can possess an orbit with certain very special properties. For example, when $K = \mathbb{C}$, Ghioca, Tucker, and Zieve [5, 6] show that if $f, g \in \mathbb{C}[x]$ with $\deg f, \deg g \geq 2$, and f has an orbit whose intersection with an orbit of g is infinite, then f and g must share a common iterate. Thus the existence of a special orbit of f has global implications for f ; in particular, it implies functional properties of the map f . Another example of such a result is due to Silverman [12, Theorem A], who shows that if $\phi \in \mathbb{Q}(z)$ and there is an orbit of ϕ containing infinitely many integers, then $\phi^2(z)$ is a polynomial (a more general result is given in [12, Theorem B]).

This theme is taken much farther in the dynamical Mordell-Lang conjecture [4], [2, Section 1.5], which posits that if Φ is an endomorphism of a quasiprojective variety X defined over \mathbb{C} , a is any point in $X(\mathbb{C})$, and $V \subset X$ is any subvariety, then $\{n \geq 0 : \Phi^n(a) \in V(\mathbb{C})\}$ is a union of finitely many arithmetic progressions (note that singletons are considered arithmetic progressions, and thus

The first and third authors' research was supported by Carleton college's HHMI grant for undergraduate science education and the Carleton college department of Mathematics and Statistics.

any finite set is a union of arithmetic progressions). In particular, if $O_\Phi(a) \cap V(\mathbb{C})$ is infinite, then V contains a positive-dimensional subvariety that is periodic under the action of f . Indeed, let $M > 0$ and $\ell \geq 0$ be such that $\Phi^{kM+\ell}(a) \in V(\mathbb{C})$ for all $k \geq 0$; then the Zariski closure of $\{\Phi^{kM+\ell}(a) : k \geq 0\}$ is positive-dimensional and invariant under Φ^M .

In this article we consider a problem similar in flavor to that of the dynamical Mordell-Lang conjecture, only we require X, Φ , and a to be defined over a number field K , and we allow V to be the value set of a K -morphism, and thus much larger than a subvariety. One of our principal results is the following:

Theorem 1.1. *Let K be a number field, let $\phi, \lambda \in K(x)$ have degree at least two, and suppose λ has two totally ramified fixed points in $\mathbb{P}^1(K)$. Then for every $a \in \mathbb{P}^1(K)$, the set $O_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is at most a finite union of sets of the form $\{\phi^{kM+\ell}(a) : k \in \mathbb{Z}_{\geq 0}\}$, where M and ℓ are non-negative integers. If $O_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is infinite, then it is the union of at most three sets of this form, each with $M \leq m$ if $m \geq 3$ and $M \leq 4$ if $m = 2$.*

In Section 10.7 we give an example where $O_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ cannot be written as a union of two arithmetic progressions, showing that three is best possible. The bound on M is best possible for $m \geq 3$, independent of K (see the remark on p. 40); for $m = 2$ the bound may not be independent of K , but $M = 4$ is realized for some K (see the discussion on p. 47). Note that when $O_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is finite, no uniform bound on its size exists. Indeed, one can specify a set $\{a_0, \dots, a_n\} \subset K$ and then use linear algebra to construct $\phi \in K(x)$ with $\phi^i(a_0) = a_i$ for $i = 0, \dots, n$. Of course, the degree of ϕ grows with n , and it may be possible to find such a uniform bound for maps of fixed degree.

Motivated in part by Theorem 1.1, we make the following arithmetic version of the dynamical Mordell-Lang conjecture:

Conjecture 1.2 (Arithmetic dynamical Mordell-Lang conjecture for \mathbb{P}^1). *Let $X = \mathbb{P}^1$ and let Y be a curve defined over a field K of characteristic zero. Suppose that $\lambda : Y \rightarrow X$ is a finite K -morphism, and $\phi : X \rightarrow X$ is a morphism of degree at least two. Then for any $a \in X(K)$, the set $\{n \geq 0 : \phi^n(a) \in \lambda(Y(K))\}$ is a finite union of arithmetic progressions.*

It is interesting to ask whether a similar conclusion holds for $X = \mathbb{P}^j$ with $j \geq 2$, where Y is a projective variety and λ is finite onto its image; indeed, one may extend the question further to the case where X and Y are any quasi-projective varieties, and ϕ is a sufficiently complicated endomorphism of X . To see why such a generalization of Conjecture 1.2 is plausible, let Z_n ($n \geq 1$) be the subvariety of $X \times X$ where the morphisms $\phi^n : X \rightarrow X$ and $\lambda : Y \rightarrow X$ agree. Suppose that $\{n \geq 0 : \phi^n(a) \in \lambda(Y(K))\}$ is infinite; otherwise the conclusion of Conjecture 1.2 holds trivially. Clearly in this case $O_\phi(a)$ cannot be finite, and hence $\phi^i(a) \neq \phi^j(a)$ for $i \neq j$. For any fixed $n \geq 1$ there are infinitely many $i > n$ with $\phi^n(\phi^{i-n}(a)) \in \lambda(Y(K))$, giving rise to infinitely many points in $Z_n(K)$. It is reasonable to expect that these points are in fact Zariski-dense in Z_n , whence the Bombieri-Lang conjecture predicts that Z_n is not a variety of general type. However, because ϕ is sufficiently complicated, its complexity should grow under iteration, forcing Z_n to be of general type unless ϕ and λ are related as functions (for instance, $f^i = \lambda \circ g$ for some K -morphism $g : X \rightarrow Y$).

The previous paragraph furnishes an outline for our proof of Theorem 1.1. In the situation of that theorem, Z_n is a curve, and thus any infinite subset is Zariski dense, and the Bombieri-Lang conjecture is the famous theorem of Faltings [8, Theorem E.0.1]. After changing coordinates so that $\lambda(y) = y^m$ for some $m \in \mathbb{Z}$ with $m \geq 2$, we write C_n instead of Z_n for the curve given by $\phi^n(x) = y^m$. We show:

Theorem 1.3. *Let K be a number field, let $\phi \in K(x)$ have degree at least two, and fix $m \geq 2$. Then the genus of $C_n : \phi^n(x) = y^m$ is bounded as $n \rightarrow \infty$ if and only if one of the following holds:*

- (1) $\phi(x) = cx^j(g(x))^m$ with $\psi(x) \in K(x)$, $0 \leq j \leq m-1$, $c \in K^*$;
- (2) $m = 4$ and $\phi(x)$ is a Lattès map of signature $(2, 4, 4)$, with $\{0, \infty\}$ in the post-critical set and $r(0) = r(\infty) = 4$;
- (3) $m = 3$ and $\phi(x)$ is a Lattès map of signature $(3, 3, 3)$, with $\{0, \infty\}$ in the post-critical set;
- (4) $m = 2$ and $\phi(x)$ is a Lattès map of signature $(2, 2, 2, 2)$ with $\{0, \infty\}$ in the post-critical set;
- (5) $m = 2$ and either $\phi(x)$ or $1/\phi(1/x)$ can be written in one of the following ways:

- (a) $-\frac{f(x)^2}{(x-C)g(x)^2}$ with $f(x)^2 + C(x-C)g(x)^2 = Cxh(x)^2$;
- (b) $-\frac{(x-C)f(x)^2}{g(x)^2}$ with $(x-C)f(x)^2 + Cg(x)^2 = xh(x)^2$;
- (c) $B\frac{(x-C)f(x)^2}{g(x)^2}$ with $B(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$;
- (d) $B\frac{x(x-C)f(x)^2}{g(x)^2}$ with $Bx(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$;

where $B, C \in K \setminus \{0\}$, $f(x), g(x), h(x) \in K[x] \setminus \{0\}$, and the numerator and denominator of each fraction have no common roots in \mathbb{C} . Moreover, in (a) we have $\deg g(x) \geq \deg f(x)$ and in (c) we have $\deg g(x) > \deg f(x)$.

Recall that the post-critical set $\text{Postcrit}(\phi)$ of a rational function $\phi \in \mathbb{C}(x)$ is $\bigcup_{n \geq 1} \phi^n(C)$, where C is the critical set for ϕ , i.e., the set of points in $\mathbb{P}^1(\mathbb{C})$ at which ϕ is not locally one-to-one. A Lattès map is a finite quotient of a self-morphism of an elliptic curve (see Section 10 for a more detailed discussion), has either three or four points in its post-critical set, and has an associated function $r(z)$ that takes the value 1 outside of $\text{Postcrit}(\phi)$ and satisfies $r(\phi(z)) = \deg_\phi(z) \cdot r(z)$ for all $z \in \mathbb{P}^1(\mathbb{C})$ (see [11, Section 4] for details). The collection of values of r on $\text{Postcrit}(\phi)$ gives the signature of ϕ .

The cases of Theorem 1.3 are not mutually exclusive; for instance, there exist Lattès maps of every signature that fall into case (1), and Lattès maps of signature $(2, 2, 2, 2)$ that fall into each of the cases in (5) (see Section 10 for more details). The maps in part (5) of Theorem 1.3 could be called *quasi-Lattès* since they have three post-critical points that behave like those of Lattès maps (or Chebyshev polynomials), but a fourth that in general does not, and indeed may have an infinite forward orbit. These maps appear not to have been studied before in general. We note that the family in (5b) includes conjugates of $-T_d(x)$ for d odd and the family in (5d) includes conjugates of $T_d(x)$ for d even, where T_d denotes the monic Chebyshev polynomial of degree d . The Lattès maps in cases (2) and (3) of Theorem 1.3 are rigid, in the sense that there are only finitely many conjugacy classes of such maps for a fixed degree d [11, Section 5]. In each such conjugacy class, up to conjugacy by a scaling there are only finitely many maps with 0 and ∞ lying in $\text{Postcrit}(\phi)$ in the required way. Hence in cases (2) and (3), ϕ is conjugate by a scaling to one of a finite set of maps. Compare to case (2) of Theorem 1.7. We note also that in cases (2)-(4), the irreducible factors of the numerator and denominator of ϕ are all defined over K (See Section 7).

A finer application of the methods used to obtain Theorem 1.3 yields:

Theorem 1.4. *Let K be a number field, let $\phi \in K(x)$ have degree at least two, and fix $m \geq 2$. Then the genus g_n of $C_n : \phi^n(x) = y^m$ is bounded as $n \rightarrow \infty$ if and only if there exist integers $r > s \geq 0$ such that $\phi^r(x) = \phi^s(x)(\psi(x))^m$ for some $\psi \in K(x)$. Moreover, we may take $r - s \leq m$ for $m \geq 3$ and $r - s \leq 4$ for $m = 2$. Finally, when g_n is bounded we have $g_n \leq 1$ for all $n \geq 1$.*

The proofs of Theorems 1.3 and 1.4 occupy most of the paper. Theorem 1.1 is easily derived from Theorem 1.4 (see Section 9).

Put $\mathbb{P}^1(K)^m = K^m \cup \{\infty\}$, and suppose that $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite. Then $C_n(K)$ is infinite for all $n \geq 1$, and by Faltings' Theorem the genus of C_n must be at most one, again for all $n \geq 1$. In particular, the genus of C_n is bounded, and Theorem 1.3 immediately gives:

Corollary 1.5. *Let $\phi \in K(x)$ have degree at least two, and fix $m \geq 2$. If there exists $a \in \mathbb{P}^1(K)$ such that $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite, then ϕ falls into one of the cases in Theorem 1.3, and ϕ satisfies the conclusion of Corollary 1.4.*

The converse of Corollary 1.5 is false, even for maps in case (1) of Theorem 1.3; see Proposition 9.1. To illustrate Corollary 1.5, consider the maps

$$\phi_1(x) = -\frac{(x+3)^2}{4x}, \quad \phi_2(x) = \frac{(x^3 + 6x^2 - 24x + 8)^3}{27x(x-2)(x^2 - 2x + 4)^3}, \quad \phi_3(x) = -\frac{9(x-4)^2}{(x-3)(3x-4)^2}.$$

The map ϕ_1 is Lattès of signature (2,4,4) and has $\{n \geq 0 : \phi_1^n(-1) \in \mathbb{P}^1(\mathbb{Q})^4\} = \{2k+1 : k \geq 0\}$ (see p. 42); the map ϕ_2 is Lattès of signature (3,3,3) and has no K -orbit with infinitely many elements of $\mathbb{P}^1(K)^3$ for $K = \mathbb{Q}$, but does have such an orbit with $K = \mathbb{Q}(\sqrt{2})$ (see p. 44); the map ϕ_3 belongs to case (5a) of Theorem 1.3, and is not Lattès and indeed not even post-critically finite, but has $\{n \geq 0 : \phi_3^n(1) \in \mathbb{P}^1(\mathbb{Q})^2\} = \{3k : k \geq 0\}$ (see p. 48).

Corollary 1.5 shows that the infinitude of $O_\phi(a) \cap \mathbb{P}^1(K)^m$ implies strong functional properties of ϕ . This theme echos the results of [5] and [12] mentioned at the beginning of this section. Theorem 1.3 makes possible other results of the same flavor, for example:

Corollary 1.6. *Let K be a number field and let $\phi \in K(x)$ have degree $d \geq 2$. Suppose that there exists $a \in \mathbb{P}^1(K)$ with $O_\phi(a) \cap \mathbb{P}^1(K)^m$ infinite, for some $m \geq 5$ with $m \mid d$. Then $\phi(x) = (\psi(x))^m$ for some $\psi \in K(x)$.*

Corollary 1.6 follows immediately from Corollary 1.5 and the observation that if $\phi(x) = c(\psi(x))^m$ with $c \notin K^m$, then for all $a \in K$, $O_\phi(a) \cap \mathbb{P}^1(K)^m \subseteq \{a\}$, and thus has at most one element.

When ϕ is a polynomial, we can give a particular concrete version of Corollary 1.5:

Corollary 1.7. *Let K be a number field, let $\phi \in K[x]$ have degree $d \geq 2$, and fix $m \geq 2$. If there exists $a \in \mathbb{P}^1(K)$ with $O_\phi(a) \cap K^m$ infinite, then one of the following holds:*

- (1) $\phi(x) = cx^j(g(x))^m$ for some $g(x) \in K[x]$, $0 \leq j \leq m-1$, and $c \in K^*$; or
- (2) $m = 2$ and ϕ is conjugate by a scaling $x \mapsto cx$ ($c \in K^*$) to

$$(1.1) \quad (-1)^d(T_d(x+2)) - 2,$$

where T_d is the degree- d monic Chebyshev polynomial.

Note that cases (1) and (2) of Corollary 1.7 are mutually exclusive, unlike the cases in Theorem 1.3. The monic Chebyshev polynomial of degree d is defined by the equation $T_d(z+z^{-1}) = z^d + z^{-d}$; see [11, Section 2] or [14, Section 6.2] for further properties. The polynomials of the form (1.1) are conjugates of T_d that contain 0 in their post-critical set but do not belong to case (1). For $d = 2, 3, 4, 5$ these maps are:

$$x(x+4) \quad - (x+4)(x+1)^2 \quad x(x+4)(x+2)^2 \quad - (x+4)(x^2+3x+1)^2.$$

For $d = 2$, Theorem 1.7 gives that a quadratic polynomial $\phi(x) \in \mathbb{Q}[x]$ has a rational orbit containing infinitely many distinct squares if and only if either

- (a.) $\phi(x)$ is the square of a linear polynomial in $\mathbb{Q}[x]$, or
- (b.) $\phi(x) = cx^2 + 4x$ with $c \in \mathbb{Q}^*$.

Necessity follows from Corollary 1.6. Sufficiency is trivial for case (a.). For maps of the form given in (b.), a simple calculation shows that $\phi^2(x) = \phi(x)(g_2(x))^2$ for some $g_2(x) \in \mathbb{Q}[x]$, and it immediately follows that $\phi^2(x) = \phi(x)(g_n(x))^2$ for some $g_n(x) \in \mathbb{Q}[x]$ for each $n \geq 1$. Hence for $a \in \mathbb{Q}$, $O_\phi(a)$ contains infinitely many squares if and only if a is the x -coordinate of a rational point on $C_2 : y^2 = cx^2 + 4x$. But the genus zero curve C_2 has the rational point $(0, 0)$, and thus infinitely many rational points. By Northcott's theorem ϕ has only finitely many rational points with finite orbits, and hence there must be a rational orbit of ϕ containing infinitely many distinct squares.

We can write the curve $C_n : \phi^n(x) = y^m$ more explicitly by choosing for each $n \geq 1$ relatively prime polynomials $p_n(x), q_n(x) \in K[x]$ with $\phi^n(x) = p_n(x)/q_n(x)$ (note that this only specifies p_n and q_n up to a common constant multiple). Then C_n is given by $p_n(x) = q_n(x)y^m$, which is birational to $y^m = p_n(x)(q_n(x))^{m-1}$. Because C_n is superelliptic, there is a direct link between its genus and the number of roots of $p_n(x)q_n(x)$ of multiplicity not divisible by m ; see section 2.1 for details. Note that the roots of $p_n(x)$ are the finite pre-images of 0 under ϕ^n (with multiplicity), and the roots of $q_n(x)$ are the finite pre-images of ∞ under ϕ^n (with multiplicity). This motivates the following definition, where $e_\psi(z)$ denotes the ramification index of a rational function ψ at $z \in \mathbb{P}^1(\mathbb{C})$.

Definition 1.8. Fix $m \geq 2$, let $\phi \in \mathbb{C}(x)$ be non-constant, and let $\alpha \in \mathbb{P}^1(\mathbb{C})$. Define $\rho_n(\alpha)$ to be the number of $z \in \phi^{-n}(\alpha)$ with $e_{\phi^n}(z)$ not divisible by m . We say that α is **m -branch abundant** for ϕ if $\rho_n(\alpha)$ is bounded as $n \rightarrow \infty$.

We conclude that the genus of C_n is bounded if and only if both 0 and ∞ are m -branch abundant points for ϕ (Corollary 2.3). We remark that in [7], the authors call $\alpha \in \mathbb{P}^1(\mathbb{C})$ *dynamically ramified* for ϕ if the set $\bigcup_{n \geq 1} \{z \in \phi^{-n}(\alpha) : e_{\phi^n}(z) = 1\}$ is finite. The definition of an m -branch abundant point is weaker in that it only considers $z \in \phi^{-n}(\alpha)$ with $m \nmid e_{\phi^n}(z)$, and moreover it only asserts a bounded number of such points as n grows, rather than finiteness of the full set of such points as n varies (although this finiteness is a corollary of our results here).

An outcome of our method is a classification, for fixed $m \geq 2$, of all rational functions with two m -branch abundant points. This is similar in some ways to the classification of rational functions with an exceptional point α , i.e., $\bigcup_{n \geq 1} \phi^{-n}(\alpha)$ is finite. Classical results in complex dynamics (see [1, Section 4.1]) show that a rational function has at most two exceptional points, and any map with an exceptional point is conjugate to a polynomial or a power map.

Theorem 1.9. Let $\phi \in \mathbb{C}(x)$ be a rational function of degree $d \geq 2$ with at least two m -branch abundant points. Then ϕ is a Lattès map of signature $(2, 4, 4)$, $(3, 3, 3)$, or $(2, 2, 2, 2)$ and $2 \leq m \leq 4$; or ϕ is conjugate to a map of one of the six forms in Table 3 (p. 28) and $m = 2$; or ϕ is conjugate to a map of the form

$$cx^j(\psi(x))^m \quad \text{with } \psi(x) \in \mathbb{C}(x), 0 \leq j \leq m-1, \text{ and } c \in \mathbb{C}^*.$$

(Note that these categories are not mutually exclusive.) Moreover, ϕ has at most four m -branch abundant points. If ϕ has four such points, then $m = 2$ and ϕ is a Lattès map of signature $(2, 2, 2, 2)$. If ϕ has three such points then either $m = 3$ and ϕ is a Lattès map of signature $(3, 3, 3)$ or $m = 2$ and ϕ is conjugate to a map of one of the forms in Table 3.

A full classification of maps possessing at least one m -branch abundant point remains out of reach at present. In Section 3 we make some progress in this direction by classifying iterated preimage structures of an m -branch abundant point when m is prime.

The methods of this article have applications to purely dynamical problems as well. For instance, it is a classical result that if $\phi \in \mathbb{C}(x)$ has an iterate that is a polynomial, then either ϕ is a polynomial

or $\phi(x) = a + b/(x - a)^d$ for some $a, b \in \mathbb{C}$ [1, Section 4.1], and in particular $\phi^2(x)$ is already a polynomial. Theorem 1.9 allows us to give a similar classification of all rational maps with an iterate that is an m th power in $\mathbb{C}(x)$. Recall that the radical $\text{rad}(m)$ of a positive integer m is the product of the distinct primes dividing m .

Corollary 1.10. *Let $m \geq 2$, and denote by $\mathbb{C}(x)^m$ the set of m th powers in $\mathbb{C}(x)$. Suppose that $\phi^n(x) \in \mathbb{C}(x)^m$ for some $n \geq 1$. Then either*

- (1) $\phi(x) = cx^j(\psi(x))^m$ for some $\psi(x) \in \mathbb{C}(x), c \in \mathbb{C}$, and $0 \leq j \leq m - 1$, where $\text{rad}(m) \mid j$; or
- (2) $m = 2$ and one of $\{\phi(x), 1/\phi(1/x)\}$ has the form

$$(1.2) \quad \frac{(x - C)f(x)^2}{g(x)^2} \quad \text{with } (x - C)f(x)^2 - Cg(x)^2 = h(x)^2,$$

where $C \in \mathbb{C} \setminus \{0\}$, $f(x), g(x), h(x) \in \mathbb{C}[x] \setminus \{0\}$, $(x - C)f(x)$ and $g(x)$ have no common roots in \mathbb{C} , and $\deg g > \deg f$.

Hence if $m \geq 3$ is squarefree, then already $\phi(x) \in \mathbb{C}(x)^m$. In general, we have $\phi^r \in \mathbb{C}(x)^m$ with

$$r = \begin{cases} 2 & \text{if } m = 2 \\ k & \text{if } m \geq 3, \end{cases}$$

where k is the largest power appearing in the prime-power factorization of m . In particular, $r \leq 1 + \log_2(m)$.

Note that maps of the form (1.2) satisfy $\phi(x) - C = h(x)^2/g(x)^2$, and so $\phi^2(x) = (\phi(x) - C)f(\phi(x))^2/g(\phi(x))^2 \in \mathbb{C}(x)^2$.

The paper is organized as follows. In Section 2 we study the genera of super-elliptic curves, and show that the genus g_n of C_n remains bounded as n grows if and only if 0 and ∞ are m -branch abundant points for ϕ (Corollary 2.3). We show that if g_n is unbounded, then it grows exponentially with n (Theorem 2.4). In section 3, we classify iterated preimage structures of an m -branch abundant point when m is prime (see Figures 1 and 2). In Section 4 we define a notion of trivial map (Definition 4.1; we characterize such maps in Proposition 6.5), and show that if $m \geq 6$ then only trivial maps can have two m -branch abundant points. In Section 5 we classify maps with two 4-branch abundant points, and show that they must be trivial or have one of two iterated preimage structures (Figure 3). In Section 6 we draw on work of Milnor (Theorems 6.1 and 6.2) and the Riemann-Hurwitz formula to turn the classification results of Sections 3, 4, and 5 into proofs of Theorems 1.9 and 1.10. In Section 7 we study the field of definition of the components of maps with two m -branch abundant points, and prove Theorem 1.7. In Section 8 we prove Theorems 1.3 and 1.4. In Section 9 we prove Theorem 1.1. Finally, in Section 10 we furnish a variety of examples of non-trivial maps with orbits possessing infinitely many distinct m th powers, showing that various quantities in Theorem 1.1 are sharp. As part of this, we give a comprehensive account of the post-critical behavior of Lattès maps. We also show that Lattès maps with certain post-critical portraits cannot be defined over \mathbb{Q} (Proposition 10.1 and Corollary 10.2) and pose questions about the field of definition of Lattès maps with a post-critical four-cycle (Questions 10.4 and 10.5).

2. m -BRANCH ABUNDANT POINTS AND THE GENUS OF C_n

For $\phi \in \mathbb{C}(z)$ recall that the ramification index $e_\phi(z)$ is the order of vanishing of ϕ at $z \in \mathbb{C}$. In particular, $e_\phi(z) > 1$ if and only if z is a critical point for ϕ . This definition may be extended to $z \in \mathbb{P}^1(\mathbb{C})$ by taking $e_\phi(\infty) = e_\psi(0)$ where $\psi(z) = 1/\phi(1/z)$. An easy argument on compositions of

power series gives the following special case of the chain rule for ramification indices (see [1, Section 2.5]):

$$(2.1) \quad e_{\phi^n}(z) = \prod_{i=0}^{n-1} e_{\phi}(\phi^i(z)),$$

and hence $e_{\phi^n}(z)$ “remembers” ramification of the map ϕ at each of $z, \phi(z), \dots, \phi^{n-1}(z)$. An essential tool throughout the present paper comes in the form of the Riemann-Hurwitz formula (see e.g. [1, Section 2.7] for a proof):

$$\sum_{z \in \mathbb{P}^1(\mathbb{C})} (e_{\phi}(z) - 1) = 2d - 2.$$

A primary goal of this section is to make precise the relationship discussed on p. 5 between the genus of $C_n : \phi^n(x) = y^m$ and m -fold ramification among points in $\phi^{-n}(0)$ and $\phi^{-n}(\infty)$. The fact that the function field $\mathbb{C}(C_n)$ is a Kummer extension of the rational function field $\mathbb{C}(x)$ plays a key role, and allows for the following explicit formula for the genus of $\mathbb{C}(C_n)$, and hence the genus of C_n . This formula is a direct consequence of [15, Proposition 3.7.3].

Proposition 2.1. *Let $\mathbb{C}(x, y)$ be the extension of $\mathbb{C}(x)$ given by $y^m = \psi(x)$, where $\psi(x) = c \prod_{i=1}^k (x - \alpha_i)^{e_i} \in \mathbb{C}(x)$ and $e_i \in \mathbb{Z} \setminus \{0\}$ for all i . Let a be the greatest positive integer dividing m and all the e_i , and put $m' = m/a$ and $e'_i = e_i/a$. Then the genus g of $\mathbb{C}(x, y)$ satisfies*

$$(2.2) \quad g = 1 + \left(\frac{k-1}{2} \right) m' - \frac{1}{2} \left(\gcd(m', e'_1 + \dots + e'_k) + \sum_{i=1}^k \gcd(m', e'_i) \right).$$

The directness of the link between the genus of $y^m = \psi(x)$ and the multiplicities of the roots and poles of $\psi(x)$ given in Proposition 2.1 is of crucial importance for our argument. This in turn relies heavily on the fact that $y^m = \psi(x)$ is super-elliptic, and thus has a function field that is a Kummer extension of $\mathbb{C}(x)$. The lack of a similar formula that holds for more general curves is a primary obstacle to the generalization of Theorem 1.1 to the case where $\lambda(x)$ is not conjugate over K to a power map.

Corollary 2.2. *Let $\mathbb{C}(x, y)$ be as in Proposition 2.1, and denote by t the number of $i \in \{1, \dots, k\}$ such that $m \nmid e_i$. If $t = 0$, then $g = 0$, and if $t > 0$ then*

$$(2.3) \quad \lceil (t/2) - 1 \rceil \leq g \leq (m-1)(t-1)/2,$$

where $\lceil \cdot \rceil$ denotes the ceiling function.

Remark. The bounds are sharp, as evidenced by the function fields of the hyperelliptic curves $y^2 = x^t - 1$.

Proof. First note that $t = 0$ if and only if $m' = 1$, and in this case (2.2) reduces to $g = 0$. Assume now that $r \geq 1$ and $m' \geq 2$. If $m \nmid e_i$, then $m' \nmid e'_i$, giving us $\gcd(m', e'_i) \leq m'/2$. From (2.2) we obtain

$$(2.4) \quad g \geq 1 + \left(\frac{k-1}{2} \right) m' - \frac{1}{2} \left(m'(1 + (k-t)) + t \frac{m'}{2} \right) = 1 + m' \left(\frac{t}{4} - 1 \right),$$

with equality if and only if $m' \mid e'_1 + \dots + e'_k$ and $\gcd(m', e'_i) = m'/2$ for each i with $m' \nmid e'_i$. Because $m' \geq 2$, (2.4) gives $g \geq (t/2) - 1$. This establishes the lower bound of (2.3) when t is even. Assume then that t is odd. Then if (2.4) is an equality, we have $\gcd(m', e'_i) = m'/2$ for an odd number of values of i and $\gcd(m', e'_i) = m'$ for the rest. Thus $e'_1 + \dots + e'_k \equiv m'/2 \pmod{m'}$, and

therefore $m' \nmid (e'_1 + \dots + e'_k)$, a contradiction. We have shown that (2.4) is a strict inequality, giving $g > (t/2) - 1$. As g is an integer, we conclude $g \geq \lceil (t/2) - 1 \rceil$.

To prove the upper bound of (2.3), note that (2.2) gives

$$g \leq 1 + \left(\frac{k-1}{2} \right) m' - \frac{1}{2} (m'(k-t) + t + 1) = \frac{(m'-1)(t-1)}{2} \leq \frac{(m-1)(t-1)}{2},$$

as desired. \square

Write $\phi^n(x) = c \prod_{i=1}^k (x - \alpha_i)^{e_i}$, and take t_n to be the number of $i \in \{1, \dots, k\}$ such that $m \nmid e_i$. Then t_n is closely related to the quantity $\rho_n(0) + \rho_n(\infty)$, where ρ_n is defined in Definition 1.8. Indeed, $\rho_n(0) + \rho_n(\infty) = t_n$ unless $\infty \in \phi^{-n}(\infty) \cup \phi^{-n}(0)$ and $m \nmid e_\phi(\infty)$, in which case $\rho_n(0) + \rho_n(\infty) = t_n + 1$. We thus obtain:

Corollary 2.3. *Let K be a number field, $\phi \in K(x)$, C_n the curve given by $\phi^n(x) = y^m$, g_n the genus of C_n , and $\rho_n(\phi) := \rho_n(0) + \rho_n(\infty)$, where $\rho_n(0)$ and $\rho_n(\infty)$ are as in Definition 1.8. Then*

$$\lceil (\rho_n(\phi) - 3)/2 \rceil \leq g_n \leq (m-1)(\rho_n(\phi) - 1)/2$$

In particular, g_n is bounded as $n \rightarrow \infty$ if and only if both 0 and ∞ are m -branch abundant for ϕ .

A consequence of Corollary 2.3 is a result on the growth rate of g_n as $n \rightarrow \infty$, where we rely in part on Theorem 1.4, which will be proved in Section 9.

Theorem 2.4. *Let K be a number field, $\phi \in K(x)$ have degree $d \geq 2$, and let g_n be the genus of the curve given by $\phi^n(x) = y^m$. Then either $g_n \geq Cd^n$ for some constant C depending only on d , or $g_n \leq 1$ for all $n \geq 1$.*

Proof of Theorem 2.4. From Corollary 2.3 we have that g_n is bounded if and only if 0 and ∞ are m -branch abundant for ϕ . From Theorem 1.4 (see Table 4 in particular), g_n is bounded if and only if $g_n \leq 1$ for all $n \geq 1$.

Suppose then that g_n is unbounded, so that $\rho_n(\phi)$ is unbounded, and without loss say that $\rho_n(0)$ is unbounded. If $\rho_n(\phi) \geq Cd^n$, then after possibly adjusting C the same conclusion holds for g_n , whence it suffices to give an exponential lower bound for $\rho_n(0)$.

Because $\rho_n(0)$ is unbounded, there is an infinite set $Z \subset \mathbb{P}^1(\mathbb{C})$ whose elements satisfy $\phi^k(z) = \alpha$ ($k \geq 1$) and $m \nmid e_{\phi^k}(z)$. Note that either α is not periodic and $O_\phi(\alpha) \cap Z = \emptyset$ or α is periodic and $O_\phi(\alpha) \cap Z$ is finite. Consider the set R of all $c \in \mathbb{C}$ with $e_\phi(c) > 1$ and $c \in O_\phi^-(\alpha)$, the backwards orbit of α . By the Riemann-Hurwitz formula, R must be finite. For each $c \in R$, $O_\phi(c) \setminus O_\phi(\alpha)$ is finite, and hence

$$\bigcup_{c \in R} O_\phi(c) = \left(\bigcup_{c \in R} (O_\phi(c) \setminus O_\phi(\alpha)) \right) \cup O_\phi(\alpha),$$

whence $\bigcup_{c \in R} O_\phi(c)$ contains only finitely many elements of Z . Therefore there exists $z \in Z$ that is not in the orbit of any ramification point of ϕ . From the definition of Z , $\phi^k(z) = \alpha$ for some $k \geq 1$. Then for all $n \geq k$, $\rho_n(0) \geq (\frac{1}{d^k})(d^n)$, furnishing the desired exponential lower bound. \square

3. CLASSIFICATION OF p -BRANCH ABUNDANT POINTS

In this section we classify the ramification structures of iterated preimages of an m -branch abundant point when $m = p$ is a prime number. We begin with a general and elementary lower bound on ramification indices.

Lemma 3.1. *Let S be a finite subset of $\mathbb{P}^1(\mathbb{C})$ with $\#S = s$, and let $\phi \in \mathbb{C}(x)$ have degree d . Let $K = \{z \in \phi^{-1}(S) : m \nmid e_\phi(z)\}$, and put $k = \#K$. Then*

$$\sum_{z \in \phi^{-1}(S)} (e_\phi(z) - 1) \geq (ds - k) \left(\frac{m-1}{m} \right),$$

where equality holds if and only if $e_\phi(z) = 1$ or m for all $z \in \phi^{-1}(S)$.

Proof. Because $\sum_{z \in \phi^{-1}(w)} e_\phi(z) = d$ for all $w \in \mathbb{C}$, we have

$$\sum_{z \in \phi^{-1}(S)} (e_\phi(z) - 1) = ds - \#(\phi^{-1}(S)).$$

Moreover, $\#(\phi^{-1}(S)) \leq k + \frac{ds-k}{m}$, where equality holds if and only if every $z \in \phi^{-1}(S)$ has ramification index equal to 1 or to m . \square

The next lemma depends crucially on the primality of p .

Lemma 3.2. *Let $\phi \in \mathbb{C}(x)$ and p be prime. Suppose that α is p^r -branch abundant for ϕ , where $r \geq 1$, and let $\beta \in \mathbb{P}^1(\mathbb{C})$ satisfy $\phi^k(\beta) = \alpha$ for some $k \geq 1$. If $p^r \nmid e_{\phi^k}(\beta)$, then β is p -branch abundant for ϕ . Furthermore, if $p \nmid e_\phi(\phi^i(\beta))$ for each $i = 0, 1, \dots, k-1$, then β is p^r -branch abundant for ϕ .*

Proof. Consider $z \in \phi^{-n}(\beta)$, implying in particular that $z \in \phi^{-(n+k)}(\alpha)$. Note that

$$(3.1) \quad e_{\phi^{n+k}}(z) = e_{\phi^k}(\phi^n(z)) \cdot e_{\phi^n}(z) = e_{\phi^k}(\beta) \cdot e_{\phi^n}(z).$$

If $p^r \nmid e_{\phi^k}(\beta)$, then (3.1) and the primality of p give

$$\#\{z \in \phi^{-n}(\beta) : p \nmid e_{\phi^n}(z)\} \leq \#\{z \in \phi^{-(n+k)}(\alpha) : p^r \nmid e_{\phi^{n+k}}(z)\}.$$

Because α is p^r -branch abundant, the right-hand side is bounded as n grows, and thus β is p -branch abundant.

If $p \nmid e_\phi(\phi^i(\beta))$ for $i = 0, 1, \dots, k-1$, then $p \nmid e_{\phi^k}(\beta)$ by (2.1), and so (3.1) and the primality of p give

$$\#\{z \in \phi^{-n}(\beta) : p^r \nmid e_{\phi^n}(z)\} = \#\{z \in \phi^{-(n+k)}(\alpha) : p^r \nmid e_{\phi^{n+k}}(z)\}.$$

Because α is p^r -branch abundant, the right-hand side is bounded as n grows, and thus β is p^r -branch abundant. \square

The next lemma is the engine behind our classification. We often apply it to a pre-image of a p -branch abundant point, and hence we use β instead of α in the statement.

Lemma 3.3. *Let $\phi \in \mathbb{C}(x)$ and p be prime, and suppose that $\beta \in \mathbb{P}^1(\mathbb{C})$ is p -branch abundant for ϕ . Let S be a finite subset of $\mathbb{P}^1(\mathbb{C})$ with $\beta \notin S$ and $\phi^k(\beta) \in S$ for some $k \geq 1$. Then there exists $y \in \mathbb{P}^1(\mathbb{C})$ satisfying the following conditions:*

- (1) $\beta \in O_\phi(y)$ (note this allows $y = \beta$).
- (2) If $n \geq 0$ is minimal such that $\phi^n(y) = \beta$, then $S \cap \{y, \phi(y), \dots, \phi^n(y)\}$ is empty.
- (3) $p \mid e_\phi(\gamma)$ for all $\gamma \in \phi^{-1}(y) \setminus S$.

Moreover, if $n \geq 1$, then $y \neq \beta$.

Proof. If each $z \in \phi^{-1}(\beta) \setminus S$ satisfies $p \mid e_\phi(z)$, then because $\beta \notin S$, we may take $y = \beta$. Otherwise, construct a (possibly finite) sequence $\gamma_1, \gamma_2, \dots$ in $\mathbb{P}^1(\mathbb{C})$ as follows. Choose $\gamma_1 \in \phi^{-1}(\beta) \setminus S$ with $p \nmid e_\phi(\gamma_1)$. If γ_i is chosen for $i \geq 1$, then select $\gamma_{i+1} \in \phi^{-1}(\gamma_i) \setminus S$ with $p \nmid e_\phi(\gamma_{i+1})$. If no such γ_{i+1} exists, then the sequence terminates with γ_i . Note that by Lemma 3.2, each γ_i is p -branch abundant for ϕ .

By construction, $\gamma_i \notin S$ for all i . Therefore all the γ_i are distinct, for if $\gamma_i = \gamma_j$ for $i > j$, then γ_i is periodic under ϕ and its orbit is $\{\gamma_i, \gamma_{i-1}, \dots, \gamma_{j+1}\}$. But $\phi^k(\beta) \in O_\phi(\gamma_i)$, and so for some $j < \ell \leq i$ we have $\gamma_\ell = \phi^k(\beta) \in S$, a contradiction.

Consider the set R of all $c \in \mathbb{P}^1(\mathbb{C})$ with $e_\phi(c) > 1$ and $O_\phi(c) \cap S \neq \emptyset$. Note that

$$(3.2) \quad \bigcup_{c \in R} O_\phi(c) \subseteq \left(\bigcup_{c \in R} (O_\phi(c) \setminus O_\phi(S)) \right) \cup O_\phi(S),$$

where $O_\phi(S) = \bigcup_{s \in S} O_\phi(s)$. Now $O_\phi(c) \setminus O_\phi(S)$ is finite, since $O_\phi(c) \cap S \neq \emptyset$. We claim that only finitely many of the γ_i lie in $O_\phi(S)$. Otherwise, the finiteness of S and the pigeonhole principle imply that infinitely many of the γ_i lie in a single orbit $O_\phi(s)$ for some $s \in S$. Because each γ_i maps into S under enough iterations of ϕ , the orbit $O_\phi(s)$ visits S infinitely often. The finiteness of S then gives $\phi^{n_1}(s) = \phi^{n_2}(s)$ for some $n_1 \neq n_2$, and hence $O_\phi(s)$ is finite, contradicting our supposition that it contains infinitely many γ_i . Now from (3.2) we have that only finitely many of the γ_i lie in $\bigcup_{c \in R} O_\phi(c)$. This implies there are only finitely many γ_i , since otherwise there is some γ_i with no ramification point of ϕ in its pre-image tree, contradicting the p -branch abundance of γ_i . Because the sequence (γ_i) is finite, we may choose its last term to be y .

To prove the last assertion of the lemma, assume $y = \beta$. Then y is periodic and $O_\phi(y) = \{y, \phi(y), \dots, \phi^{j-1}(y)\}$. But $\phi^k(\beta) \in O_\phi(y)$, and hence $O_\phi(y) \cap S \neq \emptyset$, contradicting condition (2). \square

Many of our arguments rely on ramification counting, so when we have multiple p -branch abundant points it is often crucial to know that the corresponding y given in Lemma 3.3 are distinct. We prove this in the case $k = 1$ of Lemma 3.3.

Lemma 3.4. *Let β_1, \dots, β_n be distinct p -branch abundant points for $\phi \in \mathbb{C}(x)$, and let $S \subset \mathbb{P}^1(\mathbb{C})$ be a finite set with $S \cap \{\beta_1, \dots, \beta_n\} = \emptyset$ and $\phi(\{\beta_1, \dots, \beta_n\}) \subset S$. For each $i = 1, \dots, n$, let y_i be an element satisfying the conditions of Lemma 3.3 with respect to β_i and S . Then $y_i \neq y_j$ for $i \neq j$.*

Proof. Assume to the contrary that $y_i = y_j$ for some $i \neq j$. Let $n_i \geq 0$ be minimal such that $\phi^{n_i}(y_i) = \beta_i$ and let $n_j \geq 0$ be minimal such that $\phi^{n_j}(y_j) = \beta_j$. Since $y_i = y_j$, we cannot have $n_i = n_j$, for then $\beta_i = \beta_j$. Assume without loss that $n_i > n_j$, and note that $y_i = y_j$ implies

$$\{\beta_j, \phi(\beta_j), \dots, \phi^{n_i - n_j}(\beta_j)\} = \{\phi^{n_j}(y_i), \phi^{n_j+1}(y_i), \dots, \phi^{n_i}(y_i)\} \subseteq \{y_i, \phi(y_i), \dots, \phi^{n_i}(y_i)\}.$$

But $S \cap \{y_i, \phi(y_i), \dots, \phi^{n_i}(y_i)\} = \emptyset$ by Lemma 3.3. Because $n_i - n_j \geq 1$, we have $\phi(\beta_j) \notin S$, a contradiction. \square

Another useful application of Lemma 3.3 is the following.

Lemma 3.5. *Let $\phi \in \mathbb{C}(x)$ have degree d , let p be prime, and suppose that α is p -branch abundant for ϕ . Then there exists at least one $y \in \mathbb{P}^1(\mathbb{C})$ such that $\alpha \in O_\phi(y)$ and all elements of $\phi^{-1}(y) \setminus \{\alpha\}$ have ramification index divisible by p . Moreover, every element of $\phi^{-1}(y)$ has ramification index divisible by p if and only if $p \mid d$.*

Proof. Suppose that there is some $\beta \in \phi^{-1}(\alpha)$ with $\beta \neq \alpha$ and $p \nmid e_\phi(\beta)$. Then β must be p -branch abundant by Lemma 3.2. We now apply Lemma 3.3 to β with $S = \{\alpha\}$ to find y . If there exists no such β , take $y = \alpha$.

To prove the second claim of the lemma, suppose that $\alpha \in \phi^{-1}(y)$. Because all $z \in \phi^{-1}(y) \setminus \{\alpha\}$ have ramification index divisible by p , when we reduce

$$(3.3) \quad d = \sum_{z \in \phi^{-1}(y)} e_\phi(z)$$

modulo p , we obtain $d \equiv e_\phi(\alpha) \pmod{p}$. Thus if $p \mid d$, then every member of $\phi^{-1}(y)$ has ramification index divisible by p . The other direction is immediate from (3.3). \square

With these tools in place, we now prove two results on ramification of preimages of a p -branch abundant point. We put tight limits on the number of such preimages that can have ramification index prime to p .

Theorem 3.6. *Let $\phi \in \mathbb{C}(x)$ have degree d , let p be a prime not dividing d , and suppose that α is p -branch abundant for ϕ . Then there is exactly one $z \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(z)$, α is periodic under ϕ , and $z \in O_\phi(\alpha)$.*

Proof. Because $p \nmid d$, there must be at least one $z \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(z)$. By Lemma 3.2 we have that z is p -branch abundant for ϕ and by Lemma 3.5 (with $\alpha = z$) there exists y_z such that $z \in O_\phi(y_z)$ and every element of $\phi^{-1}(y_z) \setminus \{z\}$ has ramification index divisible by p . Moreover, because $p \nmid d$, by the second statement of Lemma 3.5 we must have $z \in \phi^{-1}(y_z)$, and in particular z is periodic under ϕ . Therefore α is also periodic under ϕ , and $z \in O_\phi(\alpha)$. We claim that $\phi^{-1}(\alpha) \cap O_\phi(\alpha)$ has at most one element, which proves the lemma. Indeed, if $z_1, z_2 \in \phi^{-1}(\alpha) \cap O_\phi(\alpha)$, then α must be periodic, and both z_1 and z_2 lie in the cycle S to which α belongs. But the action of ϕ on S is one-to-one, so $\phi(z_1) = \alpha = \phi(z_2)$ implies $z_1 = z_2$. \square

Lemma 3.7. *Let $\phi \in \mathbb{C}(z)$ have degree d . Suppose that p is prime and $p \mid d$. Let α be p -branch abundant for ϕ . Then*

- (1) *if $p \geq 3$, then $\#\{z \in (\phi^{-1}(\alpha) \setminus \{\alpha\}) : p \nmid e_\phi(z)\} \leq 2$.*
- (2) *if $p = 2$, then $\#\{z \in (\phi^{-1}(\alpha) \setminus \{\alpha\}) : p \nmid e_\phi(z)\} \leq 3$.*

Proof. Suppose that $p \geq 3$, and let z_1, z_2, z_3 be distinct elements of $\phi^{-1}(\alpha) \setminus \{\alpha\}$ with $p \nmid e_\phi(z_i)$ for $i = 1, 2, 3$. By Lemma 3.2, each z_i is p -branch abundant, and so by Lemma 3.5 we can find corresponding distinct y_1, y_2 , and y_3 such that $p \mid e_\phi(w)$ for all $w \in \phi^{-1}\{y_1, y_2, y_3\}$. Write $d = qp$, and note that from Lemma 3.1 we have

$$\sum_{w \in \phi^{-1}\{y_1, y_2, y_3\}} (e_\phi(w) - 1) \geq 3q(p - 1).$$

But $2d - 2 = 2qp - 2 = 3qp - (qp + 2) < 3qp - 3q$, where the inequality follows from $p \geq 3$, and this violation of the Riemann-Hurwitz formula proves part (1) of the lemma.

Suppose now that $p = 2$, and let z_1, z_2, z_3, z_4 be distinct elements of $\phi^{-1}(\alpha) \setminus \{\alpha\}$ with $p \nmid e_\phi(z_i)$ for $i = 1, 2, 3, 4$. Note that all the z_i are 2-branch abundant. Using Lemmas 3.2 and 3.5, construct y_1, y_2, y_3, y_4 as in the previous paragraph, and note that

$$\sum_{w \in \phi^{-1}\{y_1, y_2, y_3, y_4\}} (e_\phi(w) - 1) \geq 4(d/2) = 2d.$$

This contradiction to the Riemann-Hurwitz formula proves part (2) of the lemma. \square

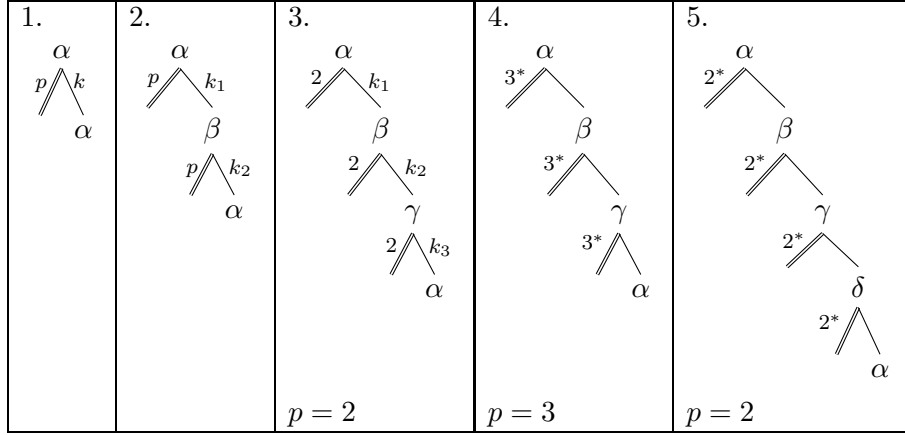


FIGURE 1. Ramification structures for $O^-(\alpha)$, where α is p -branch abundant for $f \in \mathbb{C}(z)$ and $p \nmid \deg f$. Named points are assumed to be distinct, and k_i may be any positive integer not divisible by p . A double edge with a label n denotes a set of points each of which has ramification index divisible by n . A double edge with a label n^* denotes a set of points each of which has ramification index exactly n . A single edge with a label n denotes a single point with ramification index exactly n . A single edge without a label indicates a ramification index of 1.

Theorem 3.8. *Let $\phi \in \mathbb{C}(x)$ have degree d , and let p be a prime with $p \nmid d$. Suppose that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p -branch abundant for ϕ . Then the pre-image tree T_α of α under ϕ has one of the forms given in Figure 1.*

Proof. Let ϕ be a rational function of degree $d = qp + r$, with $q, r \in \mathbb{N}$ and $1 \leq r \leq m - 1$. Let $\alpha_1 = \alpha$. By Theorem 3.6, there is a unique $\alpha_2 \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(\alpha_2)$, and so we may write $e_\phi(\alpha_2) = q_2p + r$ with $0 \leq q_2 \leq q$ and $0 < r < p$. Theorem 3.6 also guarantees that $\alpha_2 \in O_\phi(\alpha_1)$, whence $O_\phi(\alpha_2) \subseteq O_\phi(\alpha_1)$. Similarly, there is a unique $\alpha_3 \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(\alpha_3)$, and we write $e_\phi(\alpha_3) = q_3p + r$ with $0 \leq q_3 \leq q$ and note that $O_\phi(\alpha_3) \subseteq O_\phi(\alpha_2)$. Continuing in this fashion, we obtain a sequence $\alpha_1, \alpha_2, \dots$ in $\mathbb{P}^1(\mathbb{C})$ with $\phi(\alpha_{i+1}) = \alpha_i$ for all $i \geq 1$, $e_\phi(\alpha_i) = q_i p + r$ for some $q_i \leq q$, and $O_\phi(\alpha_{i+1}) \subseteq O_\phi(\alpha_i)$. By construction $\alpha_i \in O_\phi(\alpha_1)$ for each $i \geq 1$, but also α_1 is periodic and hence $O_\phi(\alpha_1)$ is finite. Thus $\alpha_i = \alpha_j$ for some $i > j$. This implies that $\alpha_1 = \alpha_{i+j-1}$. Let $n > 0$ be minimal such that $\alpha_1 = \alpha_{n+1}$. Note that the case $n = 1$ corresponds precisely to tree structure (1) in Figure 1, while the case $n = 2$ corresponds to structure (2).

Let $R = \phi^{-1}(\alpha) \setminus \{\alpha_{i+1}\}$, and recall that by Theorem 3.6 we have $p \mid e_\phi(z)$ for all $z \in R$. Now $\frac{1}{p} \sum_{z \in R} e_\phi(z) \geq \#R$, and so

$$\sum_{z \in R} (e_\phi(z) - 1) = \sum_{z \in R} e_\phi(z) - \#R \geq \left(\sum_{z \in R} e_\phi(z) \right) \left(1 - \frac{1}{p} \right),$$

Summing over i then yields

$$(3.4) \quad \sum_{i=1}^n \sum_{z \in \phi^{-1}(\alpha_i)} (e_\phi(z) - 1) \geq \sum_{i=1}^n \left[\frac{p-1}{p} (d - (q_i p + r)) + (q_i p + r - 1) \right] \\ \geq n \left(\frac{(p-1)(d-r)}{p} + (r-1) \right).$$

Suppose that $p \geq 3$. If $n \geq 3$, we have

$$n \left(\frac{(p-1)(d-r)}{p} + (r-1) \right) \geq 3 \left(\frac{2}{3} (d-r) + (r-1) \right) = 2d - 2 + (r-1).$$

Therefore we obtain a contradiction to the Riemann-Hurwitz formula unless $p = 3$ and $r = 1$. In this case, we must also have equality in (3.4), which occurs if and only if $\frac{1}{p} \sum_{z \in R} e_\phi(z) = \#R$, i.e., $e_\phi(z) = p = 3$ for all $z \in \phi^{-1}(\alpha_i) \setminus \{\alpha_i\}$ and $e_\phi(\alpha_i) = 1$ ($i = 1, 2, 3$). This is structure (4) in Figure 1.

Suppose that $p = 2$. Then $r = 1$ and

$$n \left(\frac{(p-1)(d-r)}{p} + (r-1) \right) = \frac{n}{2} (d-1).$$

We obtain a contradiction to the Riemann-Hurwitz formula unless $n \leq 4$, and when $n = 4$ we must also have equality in (3.4). The cases $n = 1$, $n = 2$, and $n = 3$ give structures (1), (2), and (3) in Figure 1, and moreover we must have k odd because $p \nmid d$. If $n = 4$, then by Lemma 3.1 we must have $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\alpha_i) \setminus \{\alpha_i\}$ ($i = 1, 2, 3, 4$) and $e_\phi(\alpha_i) = 1$. This is structure (5) in Figure 1. \square

Theorem 3.9. *Let $\phi \in \mathbb{C}(x)$ have degree d and let p be a prime dividing d . Suppose that α is p -branch abundant for ϕ . Then the pre-image tree T_α of α under ϕ has one of the forms given in Figure 2.*

Proof. For any $z \in \mathbb{P}^1(\mathbb{C})$, we define $B_z^* = \{\beta \in \phi^{-1}(z) : p \nmid e_\phi(\beta)\}$ and $B_z = B_z^* \cup \{z\}$. Let $\#B_z^* = k_z$ and $\#B_z = b_z$. To ease notation, we put $b_\alpha = b$. Lemma 3.7 shows that if $p \geq 3$ then $b \leq 2$.

If $b = 0$ for any value of p then we obtain structure (6) in Figure 2.

Case 1: Let $p \geq 3$ and $b = 2$. Then there exist $\beta_1, \beta_2 \in \phi^{-1}(\alpha)$ with ramification indices not divisible by p . Note that $\#\phi^{-1}(\alpha) \leq k_\alpha + (d - k_\alpha)/p$, and thus

$$(3.5) \quad \sum_{c \in \phi^{-1}(\alpha)} (e_\phi(c) - 1) = d - \#\phi^{-1}(\alpha) \geq (d - k_\alpha) \frac{p-1}{p} \geq (d-3) \frac{p-1}{p}.$$

Moreover, by Lemma 3.5, there are $y_1, y_2 \in \mathbb{P}^1(\mathbb{C})$ with $\beta_1 \in O_\phi(y_1)$ and $\beta_2 \in O_\phi(y_2)$ such that $p \mid e_\phi(z)$ for all $z \in \phi^{-1}(y_1) \cup \phi^{-1}(y_2)$. From Lemma 3.1 and (3.5) we thus obtain

$$(3.6) \quad \sum_{c \in \phi^{-1}(\alpha, \beta_1, \beta_2)} (e_\phi(c) - 1) \geq (d-3) \frac{p-1}{p} + (2d) \frac{p-1}{p} = 3(d-1) \left(\frac{p-1}{p} \right)$$

If $p > 3$ then this contradicts Riemann-Hurwitz. If $p = 3$ then to have equality we must have $k_\alpha = 3$ in (3.5), and so $\phi(\alpha) = \alpha$. Moreover, to obtain equality in (3.6), Lemma 3.1 ensures we must also have $e_\phi(\beta_1) = e_\phi(\beta_2) = e_\phi(\alpha) = 1$ and $e_\phi(c) = 3$ for all other members of $\phi^{-1}(\{\alpha, \beta_1, \beta_2\})$. This corresponds to structure (9) in Figure 2.

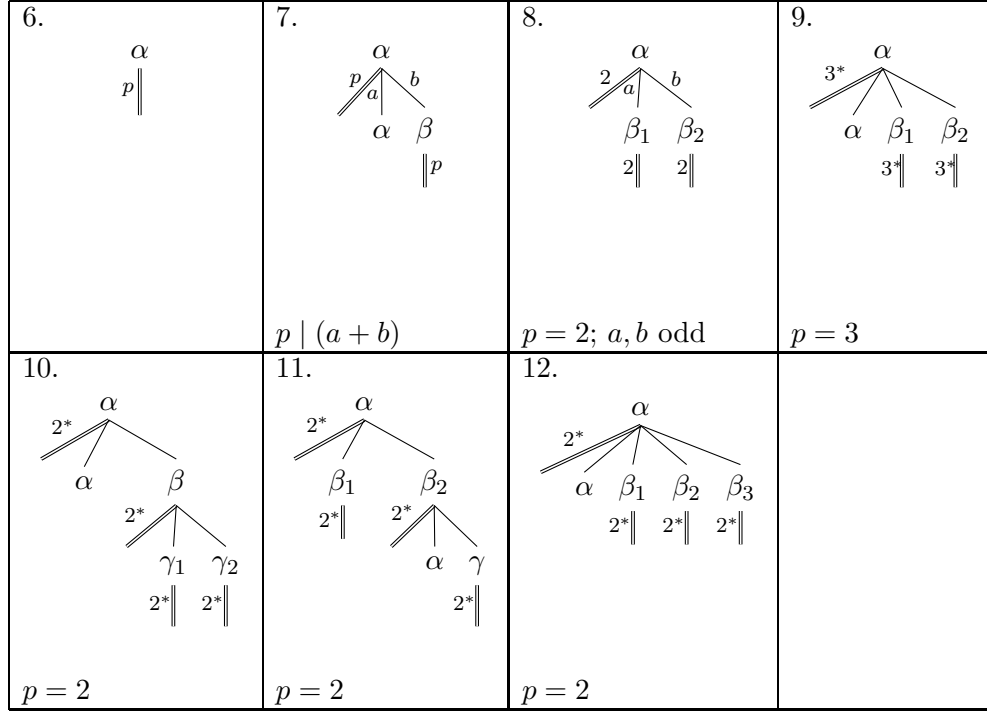


FIGURE 2. Ramification structures for $O^-(\alpha)$, where α is p -branch abundant for $\phi \in \mathbb{C}(x)$ of degree d and $p \mid d$. Notation as in Figure 1.

Case 2: Let $p \geq 3$ and $b = 1$. Note that because $p \mid d$ we cannot have $k_\alpha = 1$. Thus, $k_\alpha = 2 > b$ and so $\phi(\alpha) = \alpha$. Because $b = 1$, there exists $\beta \in \phi^{-1}(\alpha) \setminus \{\alpha\}$ such that $p \nmid e_\phi(\beta)$. From Lemma 3.2 we have that β is p -branch abundant for ϕ . By our work in case 1, $b_\beta = 2$ implies that $\phi(\beta) = \beta$, contradicting $\alpha \neq \beta$. Moreover, if $b_\beta = 1$ then because $p \mid d$ we must have $\phi(\beta) = \beta$, again a contradiction. Thus, $b_\beta = 0$, corresponding to structure (7) in Figure 2.

Case 3: Let $p = 2$ and $b = 3$. Then there are distinct $\beta_1, \beta_2, \beta_3 \in \phi^{-1}(\alpha) \setminus \{\alpha\}$, each with odd ramification index. Note that d must be at least 3, and because d is even this gives $d \geq 4$. Again because d is even, there must be a fourth element $z \in \phi^{-1}(\alpha)$ with odd ramification index, and by Lemma 3.7 we must have $z = \alpha$. In particular, $\phi(\alpha) = \alpha$.

Note that when $e_\phi(z)$ is even for all $z \in \phi^{-1}(\beta_1, \beta_2, \beta_3)$, we may apply Lemma 3.1 with $S = \{\alpha, \beta_1, \beta_2, \beta_3\}$ to obtain

$$\sum_{c \in \phi^{-1}(\{\alpha, \beta_1, \beta_2, \beta_3\})} (e_\phi(c) - 1) \geq \frac{4d - 4}{2} = 2d - 2,$$

where equality holds if and only if every member of $\phi^{-1}(\{\alpha, \beta_1, \beta_2, \beta_3\})$ has ramification index equal to 1 or 2. This corresponds to tree structure (12) in Figure 2.

Now suppose that there is $x' \in \phi^{-1}(\beta_1, \beta_2, \beta_3)$ with odd ramification index, and without loss say $\phi(x') = \beta_1$. Because $2 \mid d$, there must be $x'' \in \phi^{-1}(\beta_1)$ with $x'' \neq x'$ and $e_\phi(x'')$ odd. Note that x' and x'' are not equal to α because $\phi(\alpha) = \alpha$ and the β_i are not equal to α . By Lemma 3.5, for each of β_2, β_3, x' , and x'' we can find corresponding distinct y_2, y_3, y' , and y'' respectively such that each

element of $\phi^{-1}\{y_2, y_3, y', y''\}$ has even ramification index. Note that y_2, y_3, y', y'' are clearly distinct by Lemma 3.4. By Lemma 3.1 this gives

$$\sum_{c \in \phi^{-1}(\{y_2, y_3, y', y''\})} (e_\phi(c) - 1) \geq \frac{4d}{2} > 2d - 2,$$

contradicting Riemann-Hurwitz.

Case 4: Let $p = 2$ and $b = 2$. To handle this case, we require the following lemma.

Lemma 3.10. *Suppose that α is 2-branch abundant for ϕ and that $k_\alpha = 2$. Suppose that there exists a set $T \subset O^-(\alpha)$ of 2-branch abundant points such that $\alpha \notin T$ and $t_2 \notin O_\phi(t_1) \setminus O_\phi(\alpha)$ for all $t_1, t_2 \in T$. Then $\#T \leq 2$.*

Proof. Suppose for contradiction that there exist distinct $t_1, t_2, t_3 \in T$. By Lemma 3.5 we can find corresponding y_1, y_2 , and y_3 such that for all $i \in \{1, 2, 3\}$, $t_i \in O_\phi(y_i)$ and every member of $\phi^{-1}(y_i)$ has even ramification index.

We claim that the y_i are distinct. Indeed, by our hypothesis that $t_2 \notin O_\phi(t_1) \setminus O_\phi(\alpha)$, it is clear that if $\phi^n(t_1) = t_2$ then there exists n' such that $0 < n' < n$ and such that $\phi^{n'}(t_1) = \alpha$. Thus, by Lemma 3.4, the y_i are distinct.

Because $k_\alpha = 2$ and the y_i are distinct, we obtain from Lemma 3.1 that

$$\sum_{c \in \phi^{-1}(\alpha, y_1, y_2, y_3)} (e_\phi(c) - 1) \geq \frac{4d - 2}{2} > 2d - 2.$$

This contradicts Riemann-Hurwitz and so we have shown that $\#T \leq 2$. \square

Because $b = 2$, we have $k_\alpha = 2$ or 3. However, k_α must be even because d is, giving $k_\alpha = 2$. Let $\beta_1, \beta_2 \in \phi^{-1}(\alpha) \setminus \{\alpha\}$ with $e_\phi(\beta_1)$ and $e_\phi(\beta_2)$ both odd. By Lemma 3.7, $b_{\beta_i} \leq 3$ for $i = 1, 2$. Moreover, neither of the β_i can have $b_{\beta_i} = 3$, because then $\phi(\beta_i) = \beta_i$ by the first paragraph of Case 3, giving a contradiction. If $b_{\beta_i} = 2$ for some i (say without loss $i = 2$), then there are $x', x'' \in \phi^{-1}(\beta_2) \setminus \{\alpha\}$ with odd ramification indices. However, the set $S = \{\beta_1, x', x''\}$ satisfies the hypotheses of Lemma 3.10 and so may have at most two elements, a contradiction.

Suppose now that $b_{\beta_i} = 1$ for some i (say without loss $i = 2$), so that there is a unique $x \in \phi^{-1}(\beta_2) \setminus \{\alpha\}$ with odd ramification index. Because $k_\alpha = 2$, we must have $\alpha \in \phi^{-1}(\beta_2)$ with $e_\phi(\alpha)$ odd. Suppose that at least one member of $\phi^{-1}(x)$ has odd ramification index. Then because d is even we can find $x', x'' \in \phi^{-1}(x)$ with odd ramification indices. By applying Lemma 3.10 to the set $S = \{\beta_1, x', x''\}$ we again have a contradiction. Thus, all members of $\phi^{-1}(x)$ must have even ramification index. Note also that $b_{\beta_1} \neq 2$ by the previous paragraph, and if $b_{\beta_1} = 1$, then the fact that d is even implies $\alpha \in \phi^{-1}(\beta_1)$, which is impossible because $\phi(\alpha) = \beta_2$. Hence $b_{\beta_1} = 0$, so every element of $\phi^{-1}(\beta_1)$ has even ramification index. By Lemma 3.1 we then have

$$\sum_{c \in \phi^{-1}\{\alpha, \beta_1, \beta_2, x\}} (e_\phi(c) - 1) \geq \frac{4d - 4}{2} = 2d - 2,$$

where equality holds if and only if $e_\phi(\alpha) = e_\phi(\beta_1) = e_\phi(\beta_2) = e_\phi(x) = 1$ and all other members of $\phi^{-1}\{\alpha, \beta_1, \beta_2, x\}$ have ramification index equal to 2. This corresponds to tree structure (11) in Figure 2.

Finally, if $b_{\beta_1} = b_{\beta_2} = 0$, then we obtain structure (8) in Figure 2.

Case 5: Let $p = 2$ and $b = 1$. Then there exists a unique $\beta \in \phi^{-1}(\alpha) \setminus \{\alpha\}$ with $e_\phi(\beta)$ odd. Because d is even, we must have $\alpha \in \phi^{-1}(\alpha)$ with $e_\phi(\alpha)$ odd. Now $b_\beta \leq 3$ by Lemma 3.7, and we

cannot have $b_\beta = 1$, as the evenness of d then forces $\alpha \in \phi^{-1}(\beta)$, which is absurd. If $b_\beta = 0$, we have tree structure (6) in Figure 2.

Suppose then that $b_\beta = 2$, and let $\gamma_1, \gamma_2 \in \phi^{-1}(\beta)$ with $e_\phi(\gamma_1)$ and $e_\phi(\gamma_2)$ both odd. By the same argument given for b_β , we must have $b_{\gamma_1}, b_{\gamma_2} \in \{0, 2\}$. If at least one of the b_{γ_i} is non-zero, say without loss that $b_{\gamma_2} = 2$. Then there exist $x', x'' \in \phi^{-1}(\gamma_2)$ with $e_\phi(x')$ and $e_\phi(x'')$ both odd. The set $S = \{\gamma_1, x', x''\}$ satisfies the conditions of Lemma 3.10 and so may have at most two members, a contradiction.

Thus $b_{\gamma_1} = b_{\gamma_2} = 0$. Lemma 3.1 now gives

$$\sum_{c \in \phi^{-1}(\{\alpha, \beta, \gamma_1, \gamma_2\})} (e_\phi(c) - 1) \geq \frac{4d - 4}{2} = 2d - 2,$$

where equality holds if and only if $e_\phi(\alpha) = e_\phi(\beta) = e_\phi(\gamma_1) = e_\phi(\gamma_2) = 1$ and if all other members of $\phi^{-1}(\{\alpha, \beta, \gamma_1, \gamma_2\})$ have ramification index equal to 2. This corresponds to tree structure (10) in Figure 2. Our classification is now complete. \square

4. RATIONAL MAPS WITH TWO m -BRANCH ABUNDANT POINTS: THE $m \geq 6$ CASE

A full classification of ramification structures for a single m -branch abundant point, where m is allowed to be any integer ≥ 2 , presents complexities that put it out of reach at present. However, by Corollary 2.3, the maps of interest for this paper have *two* m -branch abundant points (which must be 0 and ∞ , though we do not use that additional information in this section). In this section we show that for $m \geq 6$, any map possessing two m -branch abundant points has a very restricted form. We introduce the following definition:

Definition 4.1. Suppose that $\phi \in \mathbb{C}(x)$ is a rational map of degree $d \geq 2$ and $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{C})$ with $\alpha_1 \neq \alpha_2$. We call ϕ **trivial with respect to** $\{\alpha_1, \alpha_2\}$ if we have $m \mid e_\phi(z)$ for all $z \in \phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2\}$.

Note that if ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$, then α_1 and α_2 are m -branch abundant for ϕ . We describe the form any trivial map must take in Lemma 6.5.

We now fix notation that will be in force throughout this section and the next. Let α_1 and α_2 be m -branch abundant points for ϕ .

- $B = \{\beta \in \mathbb{P}^1(\mathbb{C}) : \beta \notin \{\alpha_1, \alpha_2\}, \phi(\beta) \in \{\alpha_1, \alpha_2\}, m \nmid e_\phi(\beta)\}$
- $b = \#B$. Note that ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$ if and only if B is empty, i.e., $b = 0$.
- $k_i = \#\{z \in \phi^{-1}(\alpha_i) : m \nmid e_\phi(z)\}$ for $i \in \{1, 2\}$.

Because $m \nmid e_\phi(\beta)$ for each $\beta \in B$, there must be some prime p_β and some $r \geq 1$ with $p_\beta^r \mid m$ but $p_\beta^r \nmid e_\phi(\beta)$. Now clearly α_1 and α_2 are p_β^r -branch abundant, and so by Lemma 3.2, β is p_β -branch abundant. We may then apply Lemma 3.3 with $S = \{\alpha_1, \alpha_2\}$ to find for each $\beta \in B$ some y_β with $\beta \in O_\phi(y_\beta)$ and $p_\beta \mid e_\phi(z)$ for each $z \in \phi^{-1}(y_\beta) \setminus \{\alpha_1, \alpha_2\}$. Moreover, we may assume that $y_{\beta_1} \neq y_{\beta_2}$ when $\beta_1 \neq \beta_2$, for by Lemma 3.3, each y_β must map to β under iteration of ϕ before it maps into $\{\alpha_1, \alpha_2\}$. We thus set two last pieces of notation.

- $Y = \{y_\beta : \beta \in B\}$
- $\ell_Y = \#(\{\phi^{-1}(Y)\} \cap \{\alpha_1, \alpha_2\})$

Lemma 4.2. With notation as above, we have

$$(4.1) \quad b(dm - 2m + 2) + \ell_Y(m - 2) \leq 4d - 4.$$

Proof. Let p be the smallest prime dividing m , so that $p_\beta \geq p$ for all $\beta \in B$. Note that $\#\phi^{-1}(Y) \leq \ell_Y + (bd - \ell_Y)/p$, and so, by Lemma 3.1,

$$\sum_{c \in \phi^{-1}(Y)} (e_\phi(c) - 1) \geq (p - 1) \left(\frac{bd - \ell_Y}{p} \right) \geq \frac{bd - \ell_Y}{2}.$$

Note that $\phi^{-1}(\alpha_1)$ may have at most $k_1 + \frac{d-k_1}{m}$ members and so the sum of $e_\phi(c) - 1$ over $\phi^{-1}(\alpha_1)$ is at least $d - (k_1 + \frac{d-k_1}{m})$. An analogous statement holds for α_2 . Thus,

$$\begin{aligned} 2d - 2 &\geq \sum_{c \in \mathbb{P}^1(\mathbb{C})} (e_\phi(c) - 1) \geq \sum_{c \in \phi^{-1}(\{\alpha_1, \alpha_2\} \cup Y)} (e_\phi(c) - 1) \\ &\geq d - \left(k_1 + \frac{d - k_1}{m} \right) + d - \left(k_2 + \frac{d - k_2}{m} \right) + \frac{bd - \ell_Y}{2} \\ &= (2d - (k_1 + k_2)) \frac{m - 1}{m} + \frac{bd - \ell_Y}{2} \\ &\geq (2d - (b + 2 - \ell_Y)) \frac{m - 1}{m} + \frac{bd - \ell_Y}{2}, \end{aligned}$$

where the last inequality follows since $k_1 + k_2 \leq b + 2 - \ell_Y$. Multiplying through by $2m$ and regrouping terms yields the desired inequality. \square

Theorem 4.3. *Suppose that $m \geq 6$. Then every rational function with two m -branch abundant points α_1, α_2 is trivial with respect to $\{\alpha_1, \alpha_2\}$.*

Proof. The assumption that $m \geq 6$ implies that the left-hand side of (4.1) is at least $b(6d - 10) + 4\ell_Y$. If $\ell_Y \geq 1$, then this is at least $b(6d - 10) + 4$, and Lemma 4.2 gives $b(6d - 10) + 4 \leq 4d - 4$, which implies $b = 0$ since $d \geq 2$. Suppose therefore that $\ell_Y = 0$. Lemma 4.2 gives $b(6d - 10) \leq 4d - 4$, and when $d > 3$, this again shows $b = 0$.

Assume now that $\ell_Y = 0$ and $d = 3$. Because $m > d$, we must have $\phi^{-1}(\{\alpha_1, \alpha_2\}) \subset B \cup \{\alpha_1, \alpha_2\}$. Moreover, since $\ell_Y = 0$, for each $y_\beta \in Y$ all members of $\phi^{-1}(y_\beta)$ must have ramification index divisible by p_β . Because $d = 3$, we have $p_\beta = 3$ for all $\beta \in B$. Putting all this together gives

$$\sum_{c \in \phi^{-1}(\{\alpha_1, \alpha_2\})} (e_\phi(c) - 1) + \sum_{c \in \phi^{-1}(Y)} (e_\phi(c) - 1) \geq (2d - (b + 2)) + (2b) = 4 + b.$$

The Riemann-Hurwitz formula then forces $b = 0$.

Now assume $\ell_Y = 0$ and $d = 2$, so that ϕ has only two simple ramification points. Thus if $\#S > 2$ then not every point in S can be a ramification point, and hence $\#(\phi^{-1}(\{S\})) > S$. If $b \geq 1$, then there exists $\gamma_1 \in \phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2\}$. Hence for each $i > 1$, there exists $\gamma_{i+1} \in \phi^{-1}(\{\alpha_1, \alpha_2, \gamma_1, \dots, \gamma_i\}) \setminus \{\alpha_1, \alpha_2, \gamma_1, \dots, \gamma_i\}$. For each i , let n_i be minimal such that $\phi^{n_i}(\gamma_i) \in \{\alpha_1, \alpha_2\}$. For each ramification point c of ϕ , the set $O_\phi(c) \setminus (O_\phi(\alpha_1) \cup O_\phi(\alpha_2))$ is finite. Moreover, if any γ_i is in $O_\phi(\alpha_j)$ for $j = 1$ or $j = 2$, we have $O_\phi(\alpha_j) \subseteq O_\phi(\gamma_i)$ and $O_\phi(\gamma_i) \subseteq O_\phi(\alpha_j)$ and so the two sets are equal and finite. Thus, we also have that finitely many γ_i lie in $O_\phi(\alpha_1) \cup O_\phi(\alpha_2)$ and hence only finitely many of the α_i lie in the forward orbit of a ramification point. The remaining γ_i must have $m | e_\phi^{n_i}(\gamma_i)$, by the m -branch abundance of α_1 and α_2 . Choose one such γ_i and suppose, without loss that $\phi^{n_i}(\gamma_i) = \alpha_1$. By construction $\phi^j(\gamma_i) \neq \phi^k(\gamma_i)$ for all non-negative integers $j, k \leq n_i$. Now

$$m \mid e_{\phi^{n_i}}(z) = \prod_{j=0}^{n_i-1} e_\phi(\phi^j(\gamma_i)),$$

and so m must be a power of 2. Moreover, because $m \geq 6$, m must be at least 8. This means that at least three terms in the product above must have ramification index equal to 2, contradicting the fact that ϕ has only two ramification points. Hence $b = 0$ and the proof is complete. \square

5. RATIONAL MAPS WITH TWO m -BRANCH ABUNDANT POINTS: THE $m = 4$ CASE

Define B , b , k_1 , k_2 , Y , and ℓ_Y as on p. 16. For the rest of this section, suppose that $m = 4$.

Theorem 5.1. *Suppose $\phi \in \mathbb{C}(x)$ has odd degree d , and let α_1 and α_2 be distinct 4-branch abundant points for ϕ . Then ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$.*

Proof. Suppose that $2 \nmid d$. Then α_1 and α_2 are 2-branch abundant, and by the classification of 2-branch abundant points (Theorem 3.8), each must be periodic with its orbit consisting only of points with odd ramification index. If $w \in \phi^{-1}(\alpha_i)$ has ramification index divisible by 2 but not by 4, then w is 2-branch abundant and so must be periodic. But then $w \in O_\phi(\alpha_i)$, and the evenness of $e_\phi(w)$ gives a contradiction. Furthermore, again by Theorem 3.8, $\phi^{-1}(\alpha_i)$ must have a unique element with odd ramification index. Thus, there is $x_{\alpha_i} \in \phi^{-1}(\alpha_i)$ with odd ramification index such that every member of $\phi^{-1}(\alpha) \setminus \{x_\alpha\}$ has ramification index divisible by 4.

Suppose now that α_1, α_2 , and α_3 are distinct 4-branch abundant points for ϕ . By Lemma 3.1, we have

$$\sum_{c \in \phi^{-1}(\{\alpha_1, \alpha_2, \alpha_3\})} (e_\phi(c) - 1) \geq 3((d - 1) \left(\frac{3}{4}\right)) = \frac{9}{8}(2d - 2) > 2d - 2$$

Hence if α_1 and α_2 are distinct 4-branch abundant for ϕ , they are the only such points. Now x_{α_1} and x_{α_2} are also 4-branch abundant, and hence $\{x_{\alpha_1}, x_{\alpha_2}\} = \{\alpha_1, \alpha_2\}$. Therefore B is empty, proving that ϕ is trivial. \square

Lemma 5.2. *Suppose that $\phi \in \mathbb{C}(x)$ has even degree $d \geq 2$, and let α_1 and α_2 be 4-branch abundant for ϕ . Then $b \leq 1$.*

Proof. By Lemma 4.2,

$$(5.1) \quad b(4d - 6) + 2\ell_Y \leq 4d - 4$$

If $b \geq 3$, then (5.1) gives $12d - 18 + 2\ell_Y \leq 4d - 4$, or $8d + 2\ell_Y \leq 14$, which is impossible. If $b = 2$, then (5.1) gives $4d + 2\ell_Y \leq 8$, which implies $d = 2$ and $\ell_Y = 0$.

Thus suppose that $b = 2$, $d = 2$, and $\ell_Y = 0$. Because $b = 2$, we take $B = \{\beta_1, \beta_2\}$ with $\beta_1 \neq \beta_2$, and since $m > d$ we have

$$(5.2) \quad \phi^{-1}(\{\alpha_1, \alpha_2\}) \subset B \cup \{\alpha_1, \alpha_2\}.$$

The 4-branch abundance of the α_i , together with $d = 2$, implies that each β_i is 2-branch abundant. Apply Lemma 3.3 with $S = \{\alpha_1, \alpha_2\}$ to obtain $y_1, y_2 \notin S$ with $\beta_i \in O_\phi(y_i)$ for $i = 1, 2$ such that every element of $\phi^{-1}(\{y_1, y_2\}) \setminus S$ has even ramification index. By Lemma 3.4, we also have $y_1 \neq y_2$. But $\ell_Y = 0$, and thus $\phi^{-1}(\{y_1, y_2\}) \cap S$ is empty, implying that $\phi^{-1}(y_i) = \{z_i\}$ for some z_i with $e_\phi(z_i) = 2$.

Now each $z \notin \{z_1, z_2\}$ has ramification index 1. In particular, because $\{y_1, y_2\} \cap \{\alpha_1, \alpha_2\} = \emptyset$, every element of $\phi^{-1}(\alpha_i)$ has ramification index 1, for $i = 1, 2$. Hence $\#\phi^{-1}(\{\alpha_1, \alpha_2\}) = 4$, which by (5.2) forces $\{\alpha_1, \alpha_2\} \subseteq \phi^{-1}(\{\alpha_1, \alpha_2\})$ because $b = 2$. [JS Edit: Simplification]. Moreover, each β_i is 4-branch abundant, and hence each z_i is 2-branch abundant.

We claim that there can be no critical points $c \in O_\phi(z_i)$, contradicting the 2-branch abundance of the z_i . Suppose $z_1 \in O_\phi(z_1)$, then β_1 is periodic, which contradicts our construction, since the β_i

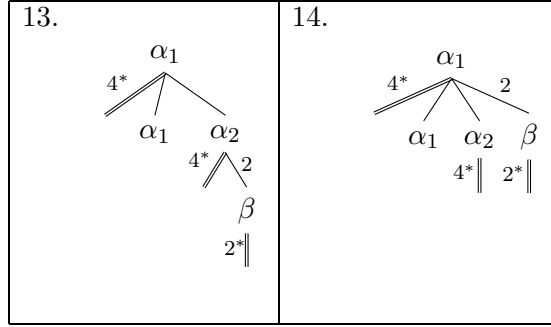


FIGURE 3. Tree diagrams for all non-trivial $\phi \in \mathbb{C}(x)$ of even degree that have two 4-branch abundant points (α_1 and α_2). Notation as in Figure 1.

are not in S , but map into S , which maps into itself. So if β_i is periodic then $\beta_i \in S$. If $z_1 \in O_\phi(z_2)$, then $O_\phi(z_1) \subset O_\phi(z_2)$, and hence $\beta_1 \in O_\phi(z_2)$. But $\beta_2 \in O_\phi(z_2)$, and therefore either $\beta_1 \in O_\phi(\beta_2)$ or $\beta_2 \in O_\phi(\beta_1)$. Again we get that one of the β_i must lie in S , a contradiction. \square

Theorem 5.3. *Suppose that $\phi \in \mathbb{C}(x)$ has even degree d and that α_1 and α_2 are distinct 4-branch abundant points for ϕ . Then ϕ is either trivial with respect to $\{\alpha_1, \alpha_2\}$ or has one of the structures in Figure 3.*

Proof. By Lemma 5.2, it suffices to consider the case $b = 1$. Suppose that $B = \{\beta\}$, and without loss of generality say $\phi(\beta) = \alpha_1$. By the definition of B ,

$$(5.3) \quad 4 \nmid e_\phi(\beta) \text{ and } 4 \mid e_\phi(z) \text{ for each } z \in \phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\beta, \alpha_1, \alpha_2\}$$

Note $\sum_{z \in \phi^{-1}(\{\alpha_1, \alpha_2\})} (e_\phi(z)) = 2d$ is divisible by 4, and hence by (5.3) we have

$$(5.4) \quad \phi(\{\alpha_1, \alpha_2\}) \cap \{\alpha_1, \alpha_2\} \neq \emptyset.$$

Without loss of generality, say that $\phi(\alpha_1) \in \{\alpha_1, \alpha_2\}$. Then summing over $c \in \phi^{-1}(\{\alpha_1, \alpha_2\})$ gives

$$(5.5) \quad \sum (e_\phi(c) - 1) = 2d - \#\phi^{-1}(\{\alpha_1, \alpha_2\}) \geq 2d - 2 - \frac{2d-2}{4} = \frac{3}{2}(d-1).$$

Suppose that $2 \nmid e_\phi(\beta)$. Applying Lemma 3.3 with $S = \{\alpha_1, \alpha_2\}$ and $p = 2$ we can find $y \notin S$ that maps to β before it maps into S , and such that $e_\phi(z)$ is even for each $z \in \phi^{-1}(y) \setminus S$. We claim that $\phi^{-1}(y) \setminus S$ is non-empty. Otherwise, we must have $\phi^{-1}(y) = \{\alpha_2\}$, since both β and α_1 map into S and $y \notin S$. This implies $e_\phi(\alpha_2) = d$ which together with (5.5) gives a contradiction to Riemann-Hurwitz. (Note that $\phi(\alpha_2) = y$ implies ramification at α_2 was not already counted in (5.5).)

Now either $4 \mid e_\phi(z)$ for each $z \in \phi^{-1}(y) \setminus S$ or $e_\phi(z) \equiv 2 \pmod{4}$ for some $z \in \phi^{-1}(y)$. In the second case z is 2-branch abundant, and we can apply Lemma 3.3 again to find y' with $z \in O_\phi(y')$ and such that every member of $\phi^{-1}(y') \setminus S$ has even ramification index. Let ℓ be the smallest positive integer so that $\phi^\ell(y') = y$. Note that by the hypotheses of Lemma 3.3 there does not exist $\ell' \leq \ell$ so that $\phi^{\ell'}(y') \in S$. Note that if $y = y'$ then y would be periodic. Because there exists no ℓ' above, $S \cap O_\phi(y)$ is empty. This is false by the construction of y and so $y \neq y'$. Take $T = \{y\}$ in the first case and $T = \{y, y'\}$ in the second case, and set

$$\ell_T = \#\phi^{-1}(T) \cap \{\alpha_1, \alpha_2\}.$$

Applying Lemma 3.1, we obtain

$$\sum_{c \in \phi^{-1}(T)} e_\phi(c) \geq \frac{3}{4}(d - \ell_T) \quad \text{and} \quad \sum_{c \in \phi^{-1}(T)} e_\phi(c) \geq \frac{2d - \ell_T}{2}$$

in the respective cases. But $(2d - \ell_T)/2 > (3d - 3\ell_T)/4$, and so we obtain a lower bound of $(3d - 3\ell_T)/4$ in both cases.

Let k_1, k_2 be as defined on p. 16, and note that (5.3) implies that $k_1 + k_2 \leq 3$. But $T \cap \{\alpha_1, \alpha_2\} = \emptyset$ by construction, so if $\alpha_i \in \phi^{-1}(T)$, then $\phi(\alpha_i) \notin \{\alpha_1, \alpha_2\}$, implying $k_1 + k_2 \leq 2$. It follows that $k_1 + k_2 + \ell_T \leq 3$. Applying Lemma 3.1 again gives

$$\sum_{c \in \phi^{-1}(Y \cup \{\alpha_1, \alpha_2\})} (e_\phi(c) - 1) \geq (d - \ell_T) \frac{3}{4} + (2d - (k_1 + k_2)) \frac{3}{4} \geq \frac{9d - 9}{4} > 2d - 2.$$

This contradiction implies that $e_\phi(\beta)$ is even, and thus $e_\phi(\beta) \equiv 2 \pmod{4}$.

We now study $\phi^{-1}(\beta)$. Define the following:

- $\ell_\beta = \#\phi^{-1}(\beta) \cap \{\alpha_1, \alpha_2\}$
- $B_\beta = \{z \in \phi^{-1}(\beta) : 2 \nmid e_\phi(z)\}$
- $b_\beta = \#B_\beta$

Note that $\ell_\beta = 2$ implies $\phi(\{\alpha_1, \alpha_2\}) = \beta \notin \{\alpha_1, \alpha_2\}$, which contradicts (5.4). By Lemma 3.2, we have that β is 2-branch abundant, and by the definition of B we have $\phi(\beta) \neq \beta$. By the classification of 2-branch abundant points for maps of even degree (Theorem 3.9), we have $\ell_\beta \in \{0, 2\}$, whence $\ell_\beta = 0$.

The 2-branch abundance of β implies that all elements of B_β are also 2-branch abundant, and the fact that $\ell_\beta = 0$ gives $B_\beta \cap \{\alpha_1, \alpha_2\} = \emptyset$. Because β is not fixed by ϕ , we have $B_\beta \cap \{\alpha_1, \alpha_2, \beta\} = \emptyset$. We may thus apply Lemma 3.3 to each $\gamma \in B_\beta$, with $p = 2$ and $S = \{\alpha_1, \alpha_2, \beta\}$ to find y_γ such that all members of $\phi^{-1}(y_\gamma) \setminus \{\alpha_1, \alpha_2, \beta\}$ have even ramification index. Because $\phi(B_\beta) \subseteq S$, Lemma 3.4 shows the y_γ are distinct. Now (5.4) implies at most one of the α_i may be in any $\phi^{-1}(y_\gamma)$, and $e_\phi(\beta)$ is even; together these give that every $z \in \phi^{-1}(y_\gamma)$ has even ramification index. Let $Y_\beta = \{y_\gamma : \gamma \in B_\beta\}$. Applying Lemma 3.1 and the fact that $k_1 + k_2 \leq 3$ then yields

$$\begin{aligned} \sum_{c \in \phi^{-1}(\{\alpha_1, \alpha_2, \beta\}) \cup Y_\beta} (e_\phi(c) - 1) &\geq (2d - (k_1 + k_2)) \frac{3}{4} + (d - b_\beta) \frac{1}{2} + b_\beta \left(\frac{d}{2}\right) \\ &\geq \frac{8d - 9}{4} + b_\beta \left(\frac{d - 1}{2}\right). \end{aligned}$$

This implies that $b_\beta = 0$, and hence all elements of $\phi^{-1}(\beta)$ have even ramification index. By Lemma 3.1, $\sum_{c \in \phi^{-1}(\beta)} (e_\phi(c) - 1) \geq \frac{d}{2}$ with equality if and only if every member of $\phi^{-1}(\beta)$ has ramification index equal to 2.

Now, from the definition of B and the fact that $B = \{\beta\}$ we have $\phi^{-1}(\{\alpha_1, \alpha_2\}) \subseteq \{\alpha_1, \alpha_2, \beta\} \cup R$, where $4 \mid e_\phi(z)$ for all $z \in R$. From $\sum_{z \in \phi^{-1}(\{\alpha_1, \alpha_2\})} e_\phi(z) = 2d$ we obtain

$$\#\phi^{-1}(\{\alpha_1, \alpha_2\}) \leq 3 + \frac{2d - 2 - e_\phi(\beta)}{4},$$

where we have equality if and only if every member of $\phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2, \beta\}$ has ramification index equal to 4 and α_1 and α_2 are in $\phi^{-1}(\{\alpha_1, \alpha_2\})$ and have ramification indices equal to 1.

Therefore

$$\begin{aligned}
\sum_{c \in \phi^{-1}(\{\alpha_1, \alpha_2, \beta\})} (e_\phi(c) - 1) &= 2d - \#(\phi^{-1}(\{\alpha_1, \alpha_2\})) + \sum_{c \in \phi^{-1}(\beta)} (e_\phi(c) - 1) \\
&\geq 2d - \left(3 + \frac{2d - 2 - e_\phi(\beta)}{4}\right) + \frac{d}{2} \\
&= 2d - 3 + \frac{2 + e_\phi(\beta)}{4} \\
&\geq 2d - 2,
\end{aligned}$$

with equality holding if and only if

- (1) $e_\phi(\beta) = 2$
- (2) $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\beta)$
- (3) $e_\phi(\alpha_1) = e_\phi(\alpha_2) = 1$
- (4) $\phi(\{\alpha_1, \alpha_2\}) \subseteq \{\alpha_1, \alpha_2\}$
- (5) $e_\phi(z) = 4$ for all $z \in \phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2, \beta\}$

In the case $d \equiv 2 \pmod{4}$, we obtain tree structure (13) in Figure 3 and in the case where $4 \mid d$ we obtain tree structure (14). \square

6. CLASSIFICATION RESULTS OVER \mathbb{C}

When ϕ has a point α with one of the ramification structures (1)-(14) given in Figures 1, 2, and 3, the ramification arising from iterated pre-images of α alone is so significant that often any other ramification would violate Riemann-Hurwitz. Indeed, let $O^-(\alpha)$ denote the backward orbit $\bigcup_{n=1}^{\infty} \phi^{-n}(\alpha)$ of $\alpha \in \mathbb{P}^1(\mathbb{C})$, and set

$$(6.1) \quad S(\alpha) := \sum_{z \in O^-(\alpha)} e_\phi(z) - 1.$$

In Table 1 we give lower bounds for $S(\alpha)$ in the cases where ϕ has a point α with one of the ramification structures given in Figures 1, 2, and 3. These lower bounds are straightforward to obtain; for instance, in structure (7), one obtains

$$S(\alpha) \geq (2d - a - b) \frac{p-1}{p} + a + b - 2 = 2(d-1) \frac{p-1}{p} + (a+b-2) \frac{1}{p},$$

which immediately gives the bound in Table 1. Note that the lower bounds in Table 1 are achieved when the points represented by the double lines in the figure are all distinct, of minimum possible multiplicity (e.g. multiplicity p when the double line is labeled with p), and all other points in the figure have multiplicity 1.

To prove Theorem 1.9, we must relate the ramification structure of backward orbits of m -branch abundant points to global properties of ϕ . When these ramification structures have certain properties, ϕ must descend from an endomorphism of an algebraic group – either \mathbb{G}_m or an elliptic curve. For this we cite some results from the invaluable paper of Milnor [11]. Recall that $z_0 \in \mathbb{P}^1(\mathbb{C})$ is called *exceptional* for ϕ if the backwards orbit $\bigcup_{n=1}^{\infty} \phi^{-n}(z_0)$ is finite.

(1)	$(d-1)\frac{p-1}{p}$	(2)	$(2d-2)\frac{p-1}{p}$
(3)	$\frac{3d-3}{2}$	(4)	$2d-2$
(5)	$2d-2$	(6)	$d\frac{p-1}{p}$
(7)	$(2d-2)\frac{p-1}{p}$	(8)	$\frac{3d-2}{2}$
(9)	$2d-2$	(10)	$2d-2$
(11)	$2d-2$	(12)	$2d-2$
(13)	$2d-2$	(14)	$2d-2$

TABLE 1. Lower bounds on $S(\alpha)$ where α is the root of a tree with ramification structures given in Figures 1, 2, and 3.

Theorem 6.1 (Milnor [11], Theorem 4.1). *Let ϕ be a rational function and \mathcal{E}_ϕ its set of exceptional points. Then ϕ is a finite quotient of an affine map¹ if and only if there exists an integer-valued function $r(z)$ on $\mathbb{P}^1(\mathbb{C})/\mathcal{E}_\phi$ satisfying $r(\phi(z)) = e_\phi(z)r(z)$.*

When ϕ is a finite quotient of an affine map, its *signature* is the sequence of values r takes on the post-critical set of ϕ . If $z \in \mathcal{E}_\phi$ then we set $r(z) = \infty$. In Theorem 4.5 and Remark 4.7 of [11], Milnor shows that there are only six possible signatures, and that the signature of a finite quotient of an affine map reveals a great deal about the map. More specifically:

Theorem 6.2 (Milnor [11]). *Let ϕ be a finite quotient of an affine map. Then ϕ is a Lattès map if and only if ϕ has signature $(2, 2, 2, 2)$, $(3, 3, 3)$, $(2, 4, 4)$, or $(2, 3, 6)$.*

The signatures $(2, 2, \infty)$ and (∞, ∞) characterize maps conjugate to Chebyshev polynomials and power maps, respectively.

We now work towards the proofs of Theorem 1.9 and Corollary 1.10. We begin by extending Theorem 4.3 to cover the $m = 5$ case.

Lemma 6.3. *Let $m \geq 5$, let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, and assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(K)$ is a set of distinct m -branch abundant points for ϕ . Then ϕ is trivial with respect to A .*

Proof. If $m \geq 6$, then the theorem follows from Theorem 4.3. Suppose that $m = 5$. By Theorems 3.8 and 3.9, the only possible ramification structures for preimages of α_1 and α_2 are (1), (2), (6), and (7) from Figures 1 and 2.

If $5 \nmid d$, then only (1) and (2) are possible. Suppose that at least one of α_1 and α_2 belongs to a diagram of type (2); without loss of generality say α_1 has this property. We now argue that α_2 must belong to the same type-(2) diagram containing α_1 , and thus lie in a two-cycle together with α_1 . If α_2 has ramification structure (1), then from Table 1 we have

$$S(\alpha_1) + S(\alpha_2) \geq \frac{4}{5}((2d-2) + (d-1)) = \frac{12}{5}d - 12/5 > 2d-2,$$

¹A rational map ϕ is a *finite quotient of an affine map* if and only if it is conjugate to either a power map, a Chebyshev polynomial, a negative Chebyshev polynomial, or a Lattès map.

where the last inequality is strict since $d \geq 2$. If α_2 has ramification structure (2) but is not in a two-cycle with α_1 , then we obtain

$$S(\alpha_1) + S(\alpha_2) \geq \frac{8}{5}(2d - 2) > 2d - 2.$$

Therefore either both α_1 and α_2 have ramification structure (1), or α_1 and α_2 form a two-cycle with ramification structure (2). In either case, every member of $\phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2\}$ has ramification index divisible by 5, and hence ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$.

If $5 \mid d$, then only (6) and (7) are possible ramification structures for α_1 and α_2 . An argument similar to that of the $5 \nmid d$ case shows that ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$. \square

Our main results classify maps $\phi \in K(x)$ for which there is $a \in K$ with $O_\phi(a) \cap \mathbb{P}^1(K)^m$ infinite. This property is invariant under conjugating ϕ by $x \mapsto 1/x$; indeed,

$$(6.2) \quad O_\phi(a) \cap \mathbb{P}^1(K)^m = O_{\phi_1}(1/a) \cap \mathbb{P}^1(K)^m$$

with $\phi_1(x) = 1/\phi(1/x)$. Thus we need only classification results up to conjugation by a particular Möbius transformation.

Theorem 6.4. *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(K)$ is a set of distinct m -branch abundant points for ϕ , and let μ be a Möbius transformation exchanging α_1 and α_2 . Suppose that ϕ is not trivial with respect to A . Then $2 \leq m \leq 4$, and for either ϕ or $\mu \circ \phi \circ \mu^{-1}$, the ramification structures of $O^-(\alpha_1)$ and $O^-(\alpha_2)$ take one of the forms specified in Table 2.*

Remark. In Table 2, the ramification structures of $O^-(\alpha_1)$ and $O^-(\alpha_2)$ are determined by the data in the column labeled “Specifications.” For ease of reference, we assign to each of these outcomes a quantity we call μ -type, which is given in the second column of Table 2.

Remark. Each of the μ -types given in Table 2 is in fact realized by a rational function defined over \mathbb{C} . Indeed, each is realized by a Lattès map; however, for a fixed number field K it is not necessarily possible to realize each μ -type. See the discussion in Section 10.

Proof. That $2 \leq m \leq 4$ follows from Lemma 6.3. If $m = 4$ then we draw on Theorems 5.1 and 5.3 to show that ϕ has μ -type (13) or (14), as given in Table 2. In the case of μ -type (13), using the notation of Figure 3, let $r(z)$ be the function $\mathbb{P}^1(\mathbb{C}) \rightarrow \mathbb{Z}$ satisfying $r(\alpha_1) = r(\alpha_2) = 4, r(\beta) = 2$, and $r(z) = 1$ otherwise. Then one easily checks that $r(\phi(z)) = e_\phi(z)r(z)$ for all $z \in \mathbb{P}^1(\mathbb{C})$, and so by Theorems 6.1 and 6.2, we have that ϕ is Lattès of signature (2,4,4). The same remarks apply to μ -type (14).

For $m \in \{2, 3\}$, we use the classification of m -branch abundant points given in Section 3. Indeed, α_1 must be the root of a tree of type (a) and α_2 must be the root of a tree of type (b), where we use the numbering of Figures 1, 2, and 3. Replacing ϕ with $\mu \circ \phi \circ \mu^{-1}$ if necessary, we assume that $a \geq b$. In the case where $a = b$ clearly it is not necessary to replace ϕ by $\mu \circ \phi \circ \mu^{-1}$ in order to obtain $a \geq b$, and so we are free to make this replacement for other purposes. Because ϕ is assumed to be non-trivial with respect to A , we must have $a \notin \{1, 6\}$.

Case 1: $m = 3$ and $3 \nmid \deg(\phi)$. If $a = 4$ then α_1 is the root of a tree of type (4). If α_2 is a named point in a disjoint diagram, then the bound in Table 1 gives an immediate violation of the Riemann-Hurwitz formula. Hence α_2 is a named point in the same diagram as α_1 , and replacing ϕ by $\mu \circ \phi \circ \mu^{-1}$ if necessary, we have $\phi(\alpha_2) = \alpha_1$, giving μ -type (4) from Table 2. It is straightforward to find a function $r(z)$ as in Theorem 6.1 and thus show that ϕ is Lattès of signature (3,3,3).

m	μ -type	Specifications	Remarks
4	(13)	α_1, α_2 as in (13)	Lattès of signature (2,4,4)
4	(14)	α_1, α_2 as in (14)	Lattès of signature (2,4,4)
3	(4)	$\alpha_2 \mapsto \alpha_1$ as part of a 3-cycle of type (4)	Lattès of signature (3,3,3)
3	(2,1)	α_1 in a 2-cycle of type (2) α_1 of type (1)	Lattès of signature (3,3,3). All critical points have multiplicity 3 (in particular $k = k_1 = k_2 = 1$)
3	(9)	$\alpha_2 \mapsto \alpha_1$ as part of structure (9)	Lattès of signature (3,3,3)
2	(5a)	$\alpha_2 \mapsto \alpha_1$ as part of a 4-cycle of type (5)	Lattès of signature (2,2,2,2)
2	(5b)	$\alpha_2 \mapsto \gamma \mapsto \alpha_1$ as part of a 4-cycle of type (5)	Lattès of signature (2,2,2,2)
2	(3,1)	α_1 in a 3-cycle of type (3) α_2 of type (1)	Lattès of signature (2,2,2,2). All critical points have multiplicity 2
2	(3)	$\alpha_2 \mapsto \alpha_1$ as part of a 3-cycle of type (3)	Not necessarily Lattès
2	(2,2)	α_1, α_2 in disjoint 2-cycles of type (2)	Same as (3,1) case
2	(2,1)	α_1 in a 2-cycle of type (2) α_2 of type (1)	Not necessarily Lattès
2	(12)	$\alpha_2 \mapsto \alpha_1$ as part of structure (12)	Lattès of signature (2,2,2,2)
2	(11a)	$\alpha_2 \mapsto \alpha_1 \mapsto \alpha_2$ as part of structure (11)	Lattès of signature (2,2,2,2)
2	(11b)	$\alpha_2 \mapsto \alpha_1 \mapsto \beta \mapsto \alpha_1$ as part of structure (11)	Lattès of signature (2,2,2,2)
2	(11c)	$\alpha_2 \mapsto \beta \mapsto \alpha_1 \mapsto \beta$ as part of structure (11)	Lattès of signature (2,2,2,2)
2	(10a)	$\alpha_2 \mapsto \alpha_1$ as part of structure (10)	Lattès of signature (2,2,2,2)
2	(10b)	$\alpha_2 \mapsto \beta \mapsto \alpha_1$ as part of structure (10)	Lattès of signature (2,2,2,2)
2	(8)	$\alpha_2 \mapsto \alpha_1$ as part of structure of type (8)	Not necessarily Lattès
2	(7,7)	α_1, α_2 in disjoint structures of type (7)	Same as (3,1) case
2	(7,6)	α_1 of type (7), α_2 disjoint of type (6)	Not necessarily Lattès

TABLE 2. Enumeration of μ -types for non-trivial maps

If $a = 2$ then α_1 is the root of a tree of type (2), and $b \leq 2$. The bounds in Table 1 preclude α_2 from being a named point in a disjoint diagram of type (2). If α_2 is a named point in a disjoint diagram of type (1), then it follows from Riemann-Hurwitz that the bounds in Table 1 must be equalities, and by the remarks on p. 21 all critical points must have multiplicity 3. One easily shows that ϕ is Lattès of signature (3,3,3). If α_2 is a named point in the diagram of type (2) that contains α_1 , then ϕ is trivial with respect to A .

Case 2: $m = 3$ and $3 \mid \deg(\phi)$. If $a = 9$ then α_1 is the root of a tree of type (9) and α_2 is a named point in a disjoint diagram, then the bound in Table 1 gives an immediate violation of the Riemann-Hurwitz formula. Hence α_2 is a named point in the same diagram as α_1 , and thus $\phi(\alpha_2) = \alpha_1$.

If $a = 7$ then α_1 is the root of a tree of type (7), and $b \in \{6, 7\}$. The bounds in Table 1 preclude α_2 from being a named point in a disjoint diagram of type (7). If α_2 is a named point in a disjoint

diagram of type (6), the bounds in Table 1 give

$$\sum_{z \in O^-(A)} (e_\phi(z) - 1) \geq S(\alpha_1) + S(\alpha_2) \geq (2d - 2)(2/3) + d(2/3) > 2d - 2,$$

violating the Riemann-Hurwitz formula. Hence α_2 is a named point in the diagram of type (7) that contains α_1 , and thus ϕ is trivial with respect to A .

Case 3: $m = 2$ and $2 \nmid \deg(\phi)$. If $a = 5$ then α_1 is the root of a tree of type (5). As in the $a = 9$ case, the bound in Table 1 and Riemann-Hurwitz force α_2 to be a named point in the same diagram as α_1 , and one easily checks that ϕ is Lattès of signature $(2,2,2,2)$. If $\phi(\alpha_i) = \alpha_j$ for $\{i, j\} = \{1, 2\}$, then replacing ϕ by its μ -conjugate if necessary, we may assume that $\phi(\alpha_2) = \alpha_1$. If $\phi(\alpha_i) \neq \alpha_j$ for $\{i, j\} = \{1, 2\}$, then we must have $\phi^2(\alpha_i) = \alpha_j$, and so we may assume that $\phi^2(\alpha_2) = \alpha_1$. These are μ -types (5a) and (5b), respectively, in Table 2.

If $a = 3$ then α_1 is the root of a tree of type (3), and $b \leq 3$. The bounds in Table 1 preclude α_2 from being a named point in a disjoint diagram of type (2) or (3). If α_2 is a fixed point in a disjoint diagram of type (1), then it follows from Riemann-Hurwitz that the bounds in Table 1 must be equalities, and by the remarks on p. 21 all critical points have multiplicity 2. One easily shows that ϕ is Lattès of signature $(2,2,2,2)$. If α_2 is a named point in the diagram of type (3) that contains α_1 , then replacing ϕ by its μ -conjugate if necessary, we may assume that $\phi(\alpha_2) = \alpha_1$.

If $a = 2$ then α_1 is the root of a tree of type (2), and $b \in \{1, 2\}$. If α_2 is a named point in a disjoint diagram of type (2), then the bounds in Table 1 must be equalities, and by the remarks on p. 21 all critical points have multiplicity 2. One easily shows that ϕ is Lattès of signature $(2,2,2,2)$. The other possibilities are that α_2 is a named point in a disjoint diagram of type (1), or α_2 is a named point in the same diagram of type (2) containing α_1 . In the latter case, ϕ is trivial with respect to A .

Case 4: $m = 2$ and $2 \mid \deg(\phi)$. If $a = 12$ then the bound in Table 1 ensures α_2 is a named point in the same diagram as α_1 , and thus $\phi(\alpha_2) = \alpha_1$. Moreover, ϕ is Lattès of signature $(2,2,2,2)$.

If $a = 11$, then again ϕ is Lattès of signature $(2,2,2,2)$ and α_2 must be a named point in the same diagram as α_1 . Using the notation of Figure 2, this leaves the possibilities $\alpha_2 = \beta_2$, $\alpha_2 = \beta_1$, and $\alpha_2 = \gamma$, which correspond respectively to μ -types (11a), (11b), and (11c) in Table 2.

If $a = 10$, then again ϕ is Lattès of signature $(2,2,2,2)$ and α_2 must be a named point in the same diagram as α_1 . The two cases $\phi(\alpha_2) = \alpha_1$ and $\phi(\alpha_2) \neq \alpha_1$ give μ -types (10a) and (10b), respectively.

If $a = 8$ then α_1 is the root of a tree of type (8), and $b \in \{6, 7, 8\}$. The bounds in Table 1 together with Riemann-Hurwitz preclude α_2 from being a named point in a disjoint diagram of type (6), (7) or (8). If α_2 is a named point in the diagram of type (8) that contains α_1 , and thus $\phi(\alpha_2) = \alpha_1$.

If $a = 7$ then α_1 is the root of a tree of type (7), and $b \in \{6, 7\}$. If α_2 is a named point in a disjoint diagram of type (7), then the bounds in Table 1 must be equalities, and by the remarks on p. 21 all critical points have multiplicity 2. One easily shows that ϕ is Lattès of signature $(2,2,2,2)$. The other possibilities are that α_2 is a named point in a disjoint diagram of type (6), or α_2 is a named point in the same diagram of type (7) containing α_1 . In the latter case, ϕ is trivial with respect to A . \square

Before we prove Theorem 1.9, we need the following result about maps that are trivial with respect to A .

Proposition 6.5. *A map $\phi \in \mathbb{C}(x)$ is trivial with respect to $\{0, \infty\}$ if and only if it is of the form*

$$(6.3) \quad cx^j(\psi(x))^m \quad \text{with } \psi(x) \in \mathbb{C}(x), 0 \leq j \leq m-1, \text{ and } c \in \mathbb{C}^*.$$

Hence if $A = \{\alpha_1, \alpha_2\}$ is any set of distinct points in $\mathbb{P}^1(\mathbb{C})$, then ϕ is trivial with respect to A if and only if it is conjugate to a map of the form (6.3).

Proof. Suppose that ϕ is trivial with respect to $\{0, \infty\}$. For each $z \in \phi^{-1}(0) \setminus \{0, \infty\}$, the factor $(x - z)$ appears in the numerator of ϕ with multiplicity $e_\phi(z)$. The same holds for $z \in \phi^{-1}(\infty) \setminus \{0, \infty\}$ and the denominator of ϕ . Letting $U = \phi^{-1}(0) \setminus \{0, \infty\}$ and $V = \phi^{-1}(\infty) \setminus \{0, \infty\}$, we can write

$$\phi(x) = c \cdot x^j \cdot \frac{\prod_{u \in U} (x - u)^m}{\prod_{v \in V} (x - v)^m}$$

for some $c \in \mathbb{C}^*$ (we cannot have $c = 0$ since ϕ is non-constant). Thus $\phi(x) = cx^j \psi(x)^m$ with $\psi(x) = \prod_{u \in U} (x - u) / \prod_{v \in V} (x - v)$. If necessary, we may absorb m th powers of x into $(\psi(x))^m$, allowing us to assume $0 \leq j \leq m - 1$.

Suppose now that $\phi(x) = cx^j (\psi(x))^m$. Then $m \mid e_{\phi(z)}$ for all $z \in \phi^{-1}(\{0, \infty\}) \setminus \{0, \infty\}$, and it follows that ϕ is trivial with respect to $\{0, \infty\}$. The last assertion of the Proposition follows by conjugating ϕ by any Möbius transformation taking A to $\{0, \infty\}$. \square

Proof of Theorem 1.9. Let $\phi \in \mathbb{C}(x)$, let $m \geq 2$, and suppose that ϕ has a set $A = \{\alpha_1, \alpha_2\}$ of distinct m -branch abundant points, and let μ be a Möbius transformation exchanging α_1 and α_2 . If ϕ is not trivial with respect to A , then Theorem 6.4 gives that $2 \leq m \leq 4$ and ϕ has one of the μ -types given in Table 2. In each case, ϕ is either Lattès of signature $(2, 4, 4)$, $(3, 3, 3)$, or $(2, 2, 2, 2)$, or of μ -type (3) , $(2, 1)$, (8) , or $(7, 6)$ (with $m = 2$). In these last four cases, ϕ has three 2-branch abundant points, and thus ϕ is conjugate to a map of one of the forms given in rows 2, 3, 5, or 6 of Table 3. This together with Proposition 6.5 proves the first assertion of Theorem 1.9.

Suppose now that ϕ has a set $A = \{\alpha_1, \alpha_2, \alpha_3\}$ of three distinct m -branch abundant points. Suppose that there is a prime $p \geq 3$ with $p \mid m$. Each of the α_i is also p -branch abundant, and from Figures 1 and 2, we may classify the possible ramification structures of the backward orbits $O^-(\alpha_i)$ for $i = 1, 2, 3$. Indeed, because of our assumption that $p \geq 3$, only six cases present themselves, which we organize into three groups:

- all three backward orbits have type (1); or one has type (1) and the other two elements of A lie in a 2-cycle of type (2);
- all three backward orbits have type (6); or one has type (6) and the other two elements of A lie in a 2-cycle of type (7);
- all three elements of A lie in a structure of type (4); all three lie in a structure of type (9).

In the first two cases, we obtain from Table 1 that

$$\sum_{z \in O^-(A)} (e_\phi(z) - 1) \geq 3(d - 1) \frac{p - 1}{p} \geq 2d - 2,$$

with equality if and only if $p = m = 3$ and all critical points have ramification index equal to 3. In this case, it is straightforward to check that there is a function $r(z)$ as in Theorem 6.1, and that ϕ is Lattès of signature $(3, 3, 3)$.

In the second two cases, we obtain from Table 1 that

$$\sum_{z \in O^-(A)} (e_\phi(z) - 1) \geq 2(d - 1) \frac{p - 1}{p} + d \frac{p - 1}{p} > 2d - 2,$$

and thus these cannot occur.

In the final two cases, we must have $p = m = 3$, and Theorems 6.1 and 6.2 show that ϕ is Lattès of signature $(3, 3, 3)$.

We now drop our assumption that m is divisible by an odd prime. Suppose that ϕ has four m -branch abundant points. Because Lattès maps of signature $(3,3,3)$ have only three 3-branch abundant points, our above analysis shows that m must be a power of 2, and thus ϕ has four 2-branch abundant points. We now obtain more cases for the ramification structures of $O^-(\alpha_i)$. We use the notation (n) to mean that ϕ has a backward orbit with ramification structure n , and the notation (n_1, n_2) to mean that ϕ has disjoint backward orbits with structures n_1 and n_2 . Note that $n = 1, 6$ involve only a single 2-branch abundant point, while $n = 2, 7$ involve two such points, $n = 3, 8$ involve three, and $n = 5, 10, 11, 12$ involve four. As before, we make three groupings:

- $\{(1), (1), (1), (1)\}, \{(2), (1), (1)\}, \{(2), (2)\}, \{(3), (1)\}, \{(7), (7)\}$
- $\{(6), (6), (6), (6)\}, \{(7), (6), (6)\}, \{(8), (6)\}$
- $\{(5)\}, \{(10)\}, \{(11)\}, \{(12)\}$

In the first two groupings, we obtain from Table 1 that

$$\sum_{z \in O^-(A)} (e_\phi(z) - 1) \geq 4(d-1) \frac{p-1}{p} = 2d-2,$$

with equality if and only if $p = m = 2$ and all critical points have ramification index equal to 2. In this case, it is straightforward to check that there is a function $r(z)$ as in Theorem 6.1, and that ϕ is Lattès of signature $(2,2,2,2)$. In the second grouping, we obtain from Table 1 that

$$\sum_{z \in O^-(A)} (e_\phi(z) - 1) \geq 2d-1,$$

and thus these cannot occur. In the final grouping, we must have $p = m = 2$, and Theorems 6.1 and 6.2 show that ϕ is Lattès of signature $(2,2,2,2)$.

We have thus shown that if an arbitrary ϕ has four m -branch abundant points, then $m = 2$ and ϕ is a Lattès map of signature $(2,2,2,2)$. On the other hand, a Lattès map of signature $(2,2,2,2)$ has precisely four 2-branch abundant points. It follows that an arbitrary ϕ can have at most four m -branch abundant points for any $m \geq 2$.

Assume now that ϕ has precisely three distinct m -branch abundant points $A = \{\alpha_1, \alpha_2, \alpha_3\}$. We have already shown that if m is not a power of two, then ϕ is a $(3,3,3)$ Lattès map. Assume then that m is a power of two, so that each of $\alpha_1, \alpha_2, \alpha_3$ is 2-branch abundant. We have six cases for the ramification structure of $O^-(A)$, which we break into groups as follows:

- (i) $\{(3)\}, \{(8)\}$
- (ii) $\{(6), (6), (6)\}, \{(7), (6)\}$
- (iii) $\{(1), (1), (1)\}, \{(2), (1)\}$

Assume that $m \geq 4$. Because α_1 and α_2 are distinct m -branch abundant points for ϕ , we may invoke Theorems 5.1 and 5.3 to conclude that ϕ is trivial with respect to some two-element subset of A , say $\{\alpha_1, \alpha_2\}$. Indeed, by Theorem 5.3, the only other possibility is that ϕ has ramification structure (13) or (14) in Table 3, but either of these implies that ϕ is Lattès of signature $(2,4,4)$, and hence cannot have three m -branch abundant points. If the preimages of A fall into group (i) above, then ϕ is not trivial with respect to any two elements of A , which gives a contradiction. For $i \in \{1, 2\}$, put

$$a_i = \begin{cases} 0 & \text{if } \alpha_i \notin \phi^{-1}(\{\alpha_1, \alpha_2\}) \\ e_\phi(\alpha_i) & \text{if } \alpha_i \in \phi^{-1}(\{\alpha_1, \alpha_2\}). \end{cases}$$

Type	ϕ	conditions	more conditions
1, 1, 1	$\frac{xf(x)^2}{g(x)^2}$	$xf(x)^2 - g(x)^2 = (x-1)h(x)^2$	$f(1)^2 = g(1)^2 = 1, \deg g \leq \deg f$
2, 1	$\frac{(x-1)f(x)^2}{g(x)^2}$	$(x-1)f(x)^2 - g(x)^2 = xh(x)^2$	$\deg g \leq \deg f$
3	$\frac{f(x)^2}{(x-1)g(x)^2}$	$f(x)^2 - (x-1)g(x)^2 = xh(x)^2$	$f(1)^2 = -1, g(1)^2 = 1, \deg g \geq \deg f$
6, 6, 6	$\frac{f(x)^2}{g(x)^2}$	$f(x)^2 - g(x)^2 = h(x)^2$	
7, 6	$\frac{x(x-1)f(x)^2}{g(x)^2}$	$x(x-1)f(x)^2 - g(x)^2 = h(x)^2$	
8	$\frac{(x-1)f(x)^2}{g(x)^2}$	$(x-1)f(x)^2 - g(x)^2 = h(x)^2$	$\deg g \geq 1 + \deg f$

TABLE 3. Normal forms of maps with exactly three 2-branch abundant points. Here $f(x), g(x), h(x) \in \mathbb{C}[x]$ are all non-zero, and the numerator and denominator of ϕ have no common roots in \mathbb{C} .

We have $m \mid e_\phi(z)$ for all $z \in \phi^{-1}(\{\alpha_1, \alpha_2\})$, and therefore

$$(6.4) \quad \sum_{z \in \phi^{-1}(\{\alpha_1, \alpha_2\})} (e_\phi(z) - 1) \geq (2d - a_1 - a_2) \frac{m-1}{m} + \max\{0, a_1 - 1\} + \max\{0, a_2 - 1\}.$$

If the backward orbits of the points in A fall into one of the cases in groups (ii) or (iii) above, then the fact that ϕ is trivial with respect to $\{\alpha_1, \alpha_2\}$ implies that α_1 and α_2 must both have type (1), both have type (6), both lie in a 2-cycle of type (2), or both lie in a 2-cycle of type (7); in all cases, α_3 must have type (1) or (6), and thus $\sum_{z \in \phi^{-1}(\alpha_3)} (e_\phi(z) - 1) \geq (d-1)/2$, and hence from (6.4) we obtain

$$\begin{aligned}
\sum_{z \in A} (e_\phi(z) - 1) &\geq (2d - a_1 - a_2) \frac{m-1}{m} + \max\{0, a_1 - 1\} + \max\{0, a_2 - 1\} + \frac{d-1}{2} \\
&\geq (2d - a_1 - a_2) \frac{3}{4} + \max\{0, a_1 - 1\} + \max\{0, a_2 - 1\} + \frac{d-1}{2} \\
&\geq 2d - 2 + \frac{3}{2} - \frac{3}{4}a_1 + \max\{0, a_1 - 1\} - \frac{3}{4}a_2 + \max\{0, a_2 - 1\} \\
&\geq 2d - 2 + \frac{3}{2} - \frac{3}{4} - \frac{3}{4} \\
&\geq 2d - 2,
\end{aligned}$$

with equality if and only if $m = 4$, every element of $\phi^{-1}(\{\alpha_1, \alpha_2\}) \setminus \{\alpha_1, \alpha_2\}$ has ramification index 4, α_3 is of type (1) and every element of $\phi^{-1}(\alpha_3) \setminus \{\alpha_3\}$ has ramification index 2, and $a_1 = a_2 = 1$. These conditions imply that ϕ is Lattès of signature (2,4,4), and hence cannot have three m -branch abundant points, a contradiction.

We have thus shown that $m = 2$. In this case each of the pre-image structures given in (i), (ii), and (iii) above is realizable. Applying a conjugation if necessary, we may assume that the 2-branch abundant points of ϕ lie at $\infty, 0$, and 1. If the three 2-branch abundant points for ϕ each have

ramification structure (1), then ϕ may be written as $Cxf(x)^2/g(x)^2$, with $g(0) \neq 0$, $\deg f \geq \deg g$, $f(1) = g(1)$, and $xf(x)^2 - g(x)^2 = b(x-1)h(x)^2$ to ensure that $0, \infty$, and 1 are fixed points with the required ramification structure. Because C and b are both squares in \mathbb{C} , we may absorb them into $f(x)$ and $h(x)$, respectively. We may divide numerator and denominator by $f(1)^2$ to ensure that $f(1)^2 = g(1)^2 = 1$. Hence ϕ has the form given in Table 3. In the case where the three 2-branch abundant points for ϕ consist of a 2-cycle of type (2) and a fixed point of type (1), we may conjugate to assume that ∞ is the fixed point and the 2-cycle consists of 0 and 1 , thereby obtaining the form given in the second row of Table 3. In the case where ϕ has a 3-cycle of type (3), we apply a conjugation if necessary to obtain $0 \mapsto 1 \mapsto \infty \mapsto 0$, giving a map of the form in Table 3. When ϕ has a fixed point of type (6) and another point of type (7), we take ∞ to be the point of type (6) and 0 to be a fixed point with 1 its only preimage of odd multiplicity. This gives the corresponding form in Table 3. When ϕ has three points with ramification structure (8), we apply a conjugation if necessary to assume that 0 has ∞ and 1 as its only preimages of odd multiplicity, and both ∞ and 1 have no preimages of odd multiplicity. This gives the corresponding form in Table 3. \square

Corollary 6.6. *Suppose that $m \geq 2$, $\phi(x) \in \mathbb{C}[x]$ has degree $d \geq 2$, and 0 is m -branch abundant for ϕ . Then one of the following holds:*

- (1) $\phi(x) = cx^j(g(x))^m$ for some $g(x) \in \mathbb{C}[x]$, $0 \leq j \leq m-1$, and $c \in \mathbb{C}^*$; or
- (2) $m = 2$ and ϕ is conjugate by a scaling $x \mapsto cx$ ($c \in \mathbb{C}^*$) to

$$(6.5) \quad (-1)^d(T_d(x+2)) - 2,$$

where T_d is the degree- d monic Chebyshev polynomial.

Proof. If ϕ is trivial with respect to $\{0, \infty\}$, then it follows from Proposition 6.5 that case (1) of the present corollary holds. Suppose then that ϕ is not trivial with respect to $\{0, \infty\}$. Because ϕ is a polynomial, ∞ is a fixed point of ϕ that is totally ramified, i.e. $e_\phi(\infty) = d$, and hence is also m -branch abundant. Lattès maps cannot have a totally ramified fixed point, for such a point would have $r(z) = \infty$ in the notation of Theorem 6.1, and hence ϕ could not have one of the signatures given in Theorem 6.2. By Theorem 1.9, we must then have that $m = 2$ and ϕ has a set of precisely three m -branch abundant points $\{0, \infty, \beta\}$, which also coincides with the post-critical set of ϕ . In the notation of Table 1, we have $S(\infty) = d-1$ and, moreover $S^-(\infty) \cap S^-(0) = \emptyset$, whence $S(0) \leq d-1$. Because ϕ is non-trivial, 0 must be the root of a tree of type (2) or (7), in which case the lower bounds given in Table 1 are equalities, and imply $S(0) = d-1$. This occurs if and only if each critical point has multiplicity 2, and all critical points of ϕ are in $\phi^{-1}(\{0, \infty, \beta\})$. Thus the function satisfying $r(0) = r(\beta) = 2$, $r(\infty) = \infty$, and $r(z) = 1$ for all z not in $\{0, \beta, \infty\}$, satisfies the conditions of Theorem 6.1. Therefore ϕ is a finite quotient of an affine map, with signature $\{2, 2, \infty\}$, whence by Theorem 6.2 it is conjugate to $\pm T_d$.

Thus let $\mu \circ \phi \circ \mu^{-1} = \pm T_d$ for some Möbius transformation μ . Conjugacy preserves signature, and hence $\mu(\infty) = \infty$ and $\mu(0) \in \{\pm 2\}$, the latter because ± 2 are the points of signature 2 for $\pm T_d$ [11, Section 2]. Hence $\mu(x) = cx \pm 2$ for some $c \in \mathbb{C}$, and we write $\mu = \mu_1 \circ \mu_2$ with $\mu_1(x) = x \pm 2$ and $\mu_2(x) = cx$.

Suppose first that d is odd. In order for the preimages of 0 under ϕ to have structure (2), 0 must lie in a 2-cycle, and hence $\mu \circ \phi \circ \mu^{-1} = -T_d$. We then have

$$(6.6) \quad (\mu_2 \circ \phi \circ \mu_2^{-1})(x) = (\mu_1^{-1} \circ -T_d \circ \mu_1)(x) = -T_d(x \pm 2) \mp 2$$

However, because d is odd, T_d is an odd function, and one easily checks that $-T_d(x-2) + 2$ is conjugate to $-T_d(x+2) - 2$ by $x \mapsto -x$, and hence from (6.6) we have that ϕ is conjugate by a scaling to $-T_d(x+2) - 2$.

If d is even, then T_d and $-T_d$ are conjugate by $x \mapsto -x$, and so replacing $\mu_2(x)$ by $-cx$ if necessary, we have $(\mu_2 \circ \phi \circ \mu_2^{-1})(x) = T_d(x \pm 2) \mp 2$. But $T_d(x - 2) + 2$ is conjugate to $T_d(x + 2) - 2$, again by $x \mapsto -x$, and so in all cases we have that ϕ is conjugate by a scaling to $T_d(x + 2) - 2$. \square

Proof of Corollary 1.10. Assume that $\phi^n(x) = (\tau(x))^m \in \mathbb{C}(x)^m$, for some $n \geq 1$. Then clearly for each $j \geq 1$ we have $\phi^{n+j}(x) = (\tau(\phi^j(x)))^m \in \mathbb{C}(x)^m$, and every $z \in \phi^{-(n+j)}(0) \cup \phi^{-(n+j)}(\infty)$ satisfies $m \mid e_\phi(z)$, so

$$(6.7) \quad \rho_{n+j}(0) = \rho_{n+j}(\infty) = 0$$

in the notation of Definition 1.8. In particular, both 0 and ∞ are m -branch abundant points for ϕ . If ϕ is trivial with respect to $\{0, \infty\}$, then by Proposition 6.5 it has the form $cx^j(\psi(x))^m$. Note then that for $n \geq 1$ we have

$$(6.8) \quad \phi^n(x) = c_n x^{j^n} (\psi_n(x))^m$$

for some $c_n \in \mathbb{C}^*$ and $\psi_n \in \mathbb{C}(x)$. Because $\phi^n(x) \in \mathbb{C}(x)^m$, we must have $m \mid j^n$, and hence $\text{rad}(m) \mid j$.

If ϕ is not trivial with respect to $\{0, \infty\}$, then taking $\mu(x) = 1/x$, we have from Theorem 6.4 that the μ -type of ϕ must be one of those given in Table 2. However, the only μ -type that leads to a non-trivial map satisfying (6.7) for all $j \geq 1$ is (8). Replacing ϕ by $\mu \circ \phi \circ \mu^{-1}$ if necessary, we may assume that 0 has only ∞ and $C \in \mathbb{C}^*$ as preimages occurring to odd multiplicity. This gives a map of the form (1.2) (compare to entry (8) in Table 3).

The last assertion of the corollary follows from (6.8) and the fact that if $\text{rad}(m) \mid j$ and k is the largest power appearing in the prime-power factorization of m , then certainly $m \mid j^k$. \square

7. FIELD OF DEFINITION OF ϕ AND ITS COMPONENTS

Many of our main results assume that ϕ is defined over a number field K . In order to prove them, we must show that various quantities in our classifications of the previous section may in fact be defined over K . The following rather general fact plays a key role in this.

Lemma 7.1. *Let F be a field of characteristic zero and \overline{F} an algebraic closure of F . Given $h(x) \in \overline{F}[x]$ and $m \geq 2$, let $g(x) \in \overline{F}[x]$ be the monic polynomial of maximal degree such that $h(x) = f(x)(g(x))^m$ for some $f(x) \in \overline{F}[x]$. If $h(x)$ has coefficients in F , then so do both $f(x)$ and $g(x)$.*

Remark. We may also define $g(x)$ to be $\prod (x - \alpha)^{e_h(\alpha)/m}$, where the product runs over all $\alpha \in \overline{F}$ with $m \mid e_h(\alpha)$. The assumption that F have characteristic zero is necessary, as illustrated by the case where ℓ is prime, $F = \mathbb{F}_\ell(t)$, $f(x) = x$, $g(x) = (x - \sqrt[\ell]{t})$, and $m = \ell$.

Proof. Let

$$\begin{aligned} R_1 &= \{\text{roots of } f \text{ that are not roots of } g\}, \\ R_2 &= \{\text{roots of } g \text{ that are not roots of } f\}, \\ R_3 &= \{\text{roots of both } f \text{ and } g\}. \end{aligned}$$

These are pairwise disjoint subsets of \overline{F} . The maximality of the degree of $g(x)$ implies that $e_h(\alpha) < m$ for each $\alpha \in R_1$, $m \mid e_h(\alpha)$ for each $\alpha \in R_2$, and each $\alpha \in R_3$ satisfies $m > e_h(\alpha)$ and $m \nmid e_h(\alpha)$. Because the set of roots of $h(x)$ is $R_1 \cup R_2 \cup R_3$ and $h(x) \in F[x]$, each $\sigma \in G_F := \text{Gal}(\overline{F}/F)$ permutes $R_1 \cup R_2 \cup R_3$. We also have $e_h(\alpha) = e_h(\sigma(\alpha))$, and it follows that $\sigma(R_i) = R_i$ for $i = 1, 2, 3$. Now the set of roots of f is $R_1 \cup R_3$, and the set of roots of g is $R_2 \cup R_3$. Let c_f be the leading coefficient of f , and observe that each of f/c_f and g are monic polynomials whose set of roots is preserved by

the action of G_F . Because F has characteristic zero, \overline{F}/F is Galois, and thus the fixed field of G_F is F , implying that f/c_f and $g(x)$ are both in $F[x]$. But c_f is the leading coefficient of $h(x)$, and thus is in F . Hence $f \in F[x]$. \square

We remark here that by definition a rational function ϕ is defined over $F(x)$ (written $\phi \in F(x)$) if there are relatively prime $p, q \in F[x]$ with $\phi = p/q$. If $\phi \in F(x)$ and $f, g \in \overline{F}[x]$ with $\phi = f/g$, then a straightforward argument shows that there is $c \in \overline{F}$ with $cf \in F[x]$ and $cg \in F[x]$. In particular, if f and g are monic then $c \in F$, and thus $f, g \in F[x]$.

Theorem 7.2. *Let F be a field of characteristic zero and $\phi \in \overline{F}(x)$. Let*

$$\psi(x) = \prod (x - \alpha)^{e_\phi(\alpha)/m},$$

where the product runs over all $\alpha \in \overline{F}$ with $m \mid e_\phi(\alpha)$. If $\phi \in F(x)$, then $\psi(x)$ and $\phi(x)/(\psi(x))^m$ are both in $F(x)$.

Proof. Assume $\phi \in F(x)$. Write $\psi(x) = g_1/g_2$, where each g_i is monic and in $\overline{F}[x]$, and $\phi(x)/(\psi(x))^m = f_1/f_2$, where each $f_i \in \overline{F}[x]$. Because $\phi(x) \in F[x]$, there is $c \in \overline{F}$ with $cf_i(x)g_i(x)^m \in F[x]$ for $i = 1, 2$. By Lemma 7.1 we have $g_i \in F[x]$ and $cf_i \in F[x]$. It follows that $\psi(x) \in F(x)$ and $\phi(x)/(\psi(x))^m \in F(x)$, the latter since $\phi(x)/(\psi(x))^m = (cf_1)/(cf_2)$. \square

Proof of Theorem 1.7. It remains to show that in case (1) of Corollary 6.6, we have $g(x) \in K[x]$ and $c \in K^*$, and in case (2) that $c \in K^*$. The claims in case (1) follow immediately from Lemma 7.1. The claim in case (2) can also be shown using Lemma 7.1, but we use a different method here. Suppose that ϕ satisfies

$$\phi(x) = (1/c)(-1)^d(T_d(cx + 2))$$

for some $c \in \mathbb{C}^*$. Since $\phi(x)$ has coefficients in K , so also $\phi''(0) \in K$. But $\phi''(0) = (1/c)(-1)^d c^2 T_d''(2)$, and so provided that the integer $T_d''(2)$ does not vanish, we have $c \in K$. Using L'Hospital's rule, one verifies that $T_d''(2) = (d^4 - d^2)/6$, and hence does not vanish for any $d \geq 2$. \square

8. PROOFS OF THEOREMS 1.3 AND 1.4

Proof of Theorems 1.3 and 1.4. By Corollary 2.3 it suffices to show that 0 and ∞ are m -branch abundant points for ϕ if and only if $\phi^r = \phi^s$ in $K(x)^*/K(x)^{*m}$ (or, for Theorem 1.3, if and only if ϕ satisfies one of conditions (1)-(5) in the statement of that theorem). Assume thus that 0 and ∞ are m -branch abundant; the other direction is trivial. Drawing on Proposition 6.5 and Theorems 6.4 and 7.2, we describe the image of ϕ^n in $K(x)^*/K(x)^{*m}$ for all $n \geq 1$. We write $K(x)^m$ for $K(x)^{*m}$ in order to ease notation. Note that the conclusions of Theorems 1.3 and 1.4 are both invariant under conjugation by $x \mapsto 1/x$. Indeed, conditions (1)-(5) in Theorem 1.3 are invariant under such conjugation, and if $\phi^r(x) = \phi^s(x)(\psi(x))^m$, then $\phi_1^r(x) = \phi_1^s(x)(\psi_1(x))^m$, where $\phi_1(x) = 1/\phi(1/x)$ and $\psi_1(x) = 1/\psi(1/x)$. Hence it suffices to consider trivial maps and maps of each μ -type (with $A = \{0, \infty\}$ and $\mu(x) = 1/x$) given in Table 2. We now show that for each of these, two properties hold: (1) $\phi^r = \phi^s$ in $K(x)/K(x)^m$ for some $r > s \geq 0$ with $r - s \leq m$ (or $r - s \leq 4$ for $m = 2$) and (2) ϕ satisfies one of conditions (1)-(5) in the statement of Theorem 1.3.

We first handle maps that are trivial with respect to $\{0, \infty\}$. By Proposition 6.5 such maps have the form $\phi(x) = cx^j(\psi(x))^m$ for $\psi(x) \in \mathbb{C}(x)$, $0 \leq j \leq m-1$ and $c \in \mathbb{C}^*$. Because $\phi \in K(x)$, we may apply Theorem 7.2 to conclude that $\psi \in K(x)$ and $c \in K^*$, and hence ϕ falls into case (1) of Theorem 1.3. Furthermore, we have

$$(8.1) \quad \phi^n(x) \equiv c^{1+j+\dots+j^{n-1}} x^{jn} \pmod{K(x)^m}$$

for $n \geq 1$. If $j = 0$ then $\phi^2(x) \equiv \phi(x) \pmod{K(x)^m}$, so let $j > 0$. We claim there are $r > s \geq 0$ with $j^{r-1} + \dots + j^s \equiv 0 \pmod{m}$ and $r - s \leq m$, which we justify in a moment. If $s = 0$, then $j^r \equiv 1 \pmod{m}$, and thus (8.1) gives $\phi^r(x) \equiv c^0 x \pmod{K(x)^m} \equiv \phi^0(x) \pmod{K(x)^m}$. If $s \geq 1$, then $1 + j + \dots + j^{r-1} \equiv 1 + j + \dots + j^{s-1} \pmod{m}$, and multiplying $j^{r-1} + \dots + j^s \equiv 0 \pmod{m}$ by $(j-1)$ gives $j^r \equiv j^s \pmod{m}$. From (8.1) we conclude $\phi^r(x) \equiv \phi^s(x) \pmod{K(x)^m}$.

To find $r > s \geq 0$ with $j^{r-1} + \dots + j^s \equiv 0 \pmod{m}$, let v_p denote the p -adic valuation, and put

$$s = \max_{p \mid \gcd(m, j)} v_p(m) \quad \text{and} \quad m' = \prod_{p \mid m, p \nmid j} p^{v_p(m)}.$$

Note that $m \mid j^s m'$ and $\gcd(j, m') = 1$. If $j = 1$, then we may take $s = 0$ and $r = m$. If $j > 1$, then let u be the order of j in $(\mathbb{Z}/m'(j-1)\mathbb{Z})^*$, so that $j^u - 1 \equiv 0 \pmod{m'(j-1)}$, and hence m' divides $(j^u - 1)/(j-1) = 1 + j + \dots + j^{u-1}$. Taking $r = s + u$ then gives $m \mid j^s(1 + j + \dots + j^{r-s-1}) = j^{r-1} + \dots + j^s$. Finally, the subgroup

$$\{g \in (\mathbb{Z}/m'(j-1)\mathbb{Z})^* : g \equiv 1 \pmod{(j-1)}\}$$

has at most m' elements and contains j , showing that $u \leq m' \leq m$. Hence $r - s \leq m$, as desired.

We now enumerate the non-trivial μ -types from Table 2, and handle each individually. We summarize our findings in Table 4. Before launching into the (lengthy) justifications for the data in this table, we show how to complete the proof of Theorem 1.4; the proof of Theorem 1.3 will be completed during the process of justifying the data in the table. First note that if ϕ has non-trivial μ -type, then Table 4 gives

$$(8.2) \quad r - s = \begin{cases} 4 & \text{if } m = 2 \text{ and } \phi \text{ has } \mu\text{-type (5a), (5b), or (11b)} \\ 3 & \text{if } m = 3 \text{ and } \phi \text{ has } \mu\text{-type (4)} \\ 3 & \text{if } m = 2 \text{ and } \phi \text{ has } \mu\text{-type (3,1) or (3)} \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases}$$

In particular, we have $r - s \leq m$ for $m \geq 3$ and $r - s \leq 4$ if $m = 2$. Now let g_n denote the genus of the curve $C_n : y^m = \phi^n(x)$; we show that $g_n \leq 1$ for all $n \geq 1$. Clearly if $\phi^n(x) \equiv r_n(x) \pmod{K(x)^{*m}}$, then $\mathbb{C}(\sqrt[m]{\phi^n(x)}) = \mathbb{C}(\sqrt[m]{r_n(x)})$, and so the genus of C_n is the same as that of $y^m = r_n(x)$. If ϕ is trivial, then we may take $r_n(x) = x^{j^n \bmod m}$ as in (8.1), and it follows from Proposition 2.1 that $g_n = 0$ for all $n \geq 1$. Otherwise, from Table 4, if $m = 4$ then we may take $r_n(x) = cx^3(x - \beta)^2$ for some $c \in \mathbb{C}$, and from Proposition 2.1 we have $g_n = 1$ for all $n \geq 1$. If $m = 3$, then $g_n = 0$ for all $n \geq 1$ if ϕ has μ -type (4) or (2,1) and $g_n = 1$ for all $n \geq 1$ if ϕ has μ -type (9). If $m = 2$ we have all $g_n = 0$ for μ -types (5a), (5b), (3,1), (3), (2,2), (2,1), (11b), (11c), (8), and (7,6); and all $g_n = 1$ for μ -types (12), (11a), (10a), and (7,7). This leaves us with $m = 2$ and μ -type (10b), which is the only case where g_n is non-constant: $g_1 = 0$ and $g_n = 1$ for $n \geq 2$.

Justifications for the data in Table 4:

$m = 4$, μ -type (13): We describe this computation in some detail, and then omit similar details in the remaining cases. From Theorem 6.4, ϕ is Lattès of signature (2,4,4) with 0 and ∞ being points of signature 4, and hence satisfies case (2) of Theorem 1.3. Given that ϕ has ramification structure (13) in Figure 3 we may assume without loss that $\alpha_1 = \infty$ and $\alpha_2 = 0$. The pre-images of ∞ are 0, ∞ , and points of ramification degree divisible by 4. Thus the denominator of ϕ has the form $C_1 x g(x)^4$ for some $C_1 \in \mathbb{C}$ and monic $g \in \mathbb{C}[x]$. Similarly, the numerator has the form $C_2 (x - \beta)^2 f(x)^4$ for $C_2 \in \mathbb{C}$ and monic $f \in \mathbb{C}[x]$ with $\gcd(f, g) = 1$. By Theorem 7.2 and the remark before it, we may

m	μ -type	image of $\phi^n(x)$ in $K(x)^*/K(x)^{*m}$ (note $\phi^0(x) = x$)
4	(13)	$\phi(x) \equiv Mx^3(x-\beta)^2, \quad \phi^2(x) \equiv x^3(x-\beta)^2, \quad \phi^3(x) \equiv \phi(x)$
4	(14)	$\phi(x) \equiv Mx^3(x-\beta)^2, \quad \phi^2(x) \equiv x^3(x-\beta)^2, \quad \phi^3(x) \equiv \phi(x)$
3	(4)	$\phi(x) \equiv \gamma x^2(x-\gamma), \quad \phi^2(x) \equiv \gamma^2(x-\gamma)^2, \quad \phi^3(x) \equiv x$
3	(2, 1)	$\phi(x) \equiv (x-\beta), \quad \phi^2(x) \equiv x$
3	(9)	$\phi(x) \equiv x^2(x-\beta)^2, \quad \phi^2(x) \equiv \phi(x)$
2	(5a)	$\phi(x) \equiv \delta x(x-\gamma), \quad \phi^2(x) \equiv \gamma(x-\gamma)(x-\delta),$ $\phi^3(x) \equiv -\gamma\delta(x-\delta), \quad \phi^4(x) \equiv x$
2	(5b)	$\phi(x) \equiv \delta(x-\gamma)(x-\delta), \quad \phi^2(x) \equiv \gamma\delta x,$ $\phi^3(x) \equiv \gamma(x-\gamma)(x-\delta), \quad \phi^4(x) \equiv x$
2	(3, 1)	$\phi(x) \equiv (x-\beta), \quad \phi^2(x) \equiv x-\gamma, \quad \phi^3(x) \equiv x$
2	(3)	$\phi(x) \equiv -(x-C), \quad \phi^2(x) \equiv Cx(x-C), \quad \phi^3(x) \equiv x$
2	(2, 2)	$\phi(x) \equiv \beta_1(x-\beta_1)(x-\beta_2), \quad \phi^2(x) \equiv x$
2	(2, 1)	$\phi(x) \equiv -x(x-C), \quad \phi^2(x) \equiv x$
2	(12)	$\phi(x) \equiv Mx(x-\beta_1)(x-\beta_2), \quad \phi^2(x) \equiv x(x-\beta_1)(x-\beta_2), \quad \phi^3(x) \equiv \phi(x)$
2	(11a)	$\phi(x) \equiv x(x-\beta)(x-\gamma), \quad \phi^2(x) \equiv \phi(x)$
2	(11b)	$\phi(x) \equiv \beta x(x-\beta), \quad \phi^2(x) \equiv -\beta\gamma(x-\gamma),$ $\phi^3(x) \equiv -\gamma x(x-\beta), \quad \phi^4(x) \equiv x-\gamma, \quad \phi^5(x) \equiv \phi(x)$
2	(11c)	$\phi(x) \equiv \beta(x-\beta)(x-\gamma), \quad \phi^2(x) \equiv x$
2	(10a)	$\phi(x) \equiv -x(x-\gamma_1)(x-\gamma_2), \quad \phi^2(x) \equiv x(x-\gamma_1)(x-\gamma_2), \quad \phi^3(x) \equiv \phi(x)$
2	(10b)	$\phi(x) \equiv -(x-\beta), \quad \phi^2(x) \equiv x(x-\beta)(x-\gamma),$ $\phi^3(x) \equiv -x(x-\beta)(x-\gamma), \quad \phi^4(x) \equiv \phi^2(x)$
2	(8)	$\phi(x) \equiv B(x-C), \quad \phi^2(x) \equiv -BC, \quad \phi^3(x) \equiv \phi^2(x)$
2	(7, 7)	$\phi(x) \equiv x(x-\beta_1)(x-\beta_2), \quad \phi^2(x) \equiv \phi(x)$
2	(7, 6)	$\phi(x) \equiv Bx(x-C), \quad \phi^2(x) \equiv -Cx(x-C), \quad \phi^3(x) \equiv \phi(x)$

TABLE 4. $\phi^n \pmod{K(x)^{*m}}$ for non-trivial μ -types.

take $f, g \in K[x]$ and $C_1, C_2 \in K$. Setting $M = C_2/C_1$ gives

$$(8.3) \quad \phi(x) = M \frac{(x-\beta)^2 f(x)^4}{xg(x)^4} \equiv M \frac{(x-\beta)^2}{x} \pmod{K(x)^4}.$$

Hence $\phi^2(x) \equiv M(\phi(x) - \beta)^2/\phi(x) \pmod{K(x)^m}$, and so we must calculate $\phi(x) - \beta$:

$$(8.4) \quad \phi(x) - \beta = \frac{M}{xg(x)^4} [(x-\beta)^2 f(x)^4 - (\beta/M)xg(x)^4].$$

The roots (with multiplicity) of the polynomial in square braces are the preimages (with multiplicity) of β under ϕ , and hence the polynomial in square braces equals $bh(x)^2$, with $b, h(x) \in \mathbb{C}[x]$ non-zero. Applying Theorem 7.2 again, we have $b, h(x) \in K[x]$. Putting $x = \beta$ in this polynomial, squaring, and using that $g(\beta) \neq 0$ (otherwise $\phi(\beta) \neq 0$, contrary to supposition), we have $M^2 b^2 \in K^4$. Similarly, putting $x = 0$ yields $b^2 \in K^4$, and hence $M^2 \in K^4$. It follows from (8.4) that $\phi(x) - \beta \in \frac{Mb}{x} K(x)^2$,

and thus $(\phi(x) - \beta)^2 \in \frac{1}{x^2}K(x)^4$. Returning to (8.3) now gives

$$\phi^2(x) \equiv M \frac{(\phi(x) - \beta)^2}{\phi(x)} \equiv \frac{1}{x(x - \beta)^2} \equiv x^3(x - \beta)^2 \pmod{K(x)^4}.$$

Similarly, we have

$$\phi^3(x) \equiv \frac{1}{\phi(x)(\phi(x) - \beta)^2} \equiv \frac{M^3 x^3}{(x - \beta)^2} \equiv \frac{M x^3}{(x - \beta)^2} \equiv \frac{M(x - \beta)^2}{x} \equiv \phi(x) \pmod{K(x)^4}.$$

Remark. Theorem 7.2 is frequently applied in subsequent cases to show that relevant polynomials and constants are defined over K . Hence *from now on we assume that f and g are relatively prime polynomials with coefficients in K , and that $b, b_1, b_2 \in K$ and $h, h_1, h_2 \in K[x]$ are non-zero.*

Remark. We have chosen the letter M in the above because $1/M$ is the multiplier of the (simple) fixed point ∞ of ϕ . Arithmetic properties of M are well-understood. Indeed by [11, Corollary 3.9], the multiplier at any fixed point of ϕ has the form $(\omega a)^s$, where $a \in R$ is the derivative of the linear map of which ϕ is a quotient (see Section 10.1), R is the ring of integers in an imaginary quadratic number field (indeed R is the endomorphism ring of the underlying elliptic curve), s is the signature of the fixed point in question, and $\omega^n = 1$, where $n \in \{2, 3, 4, 6\}$ is determined by ϕ (see Section 10.1). From Table 2 we have that in all cases where ϕ is Lattès and ∞ is an m -branch abundant fixed point, ∞ is a point of signature $s = m$. Moreover, it follows from Section 10.1 that either $n = m$ or $n = 6$ and $m = 3$. But in this last case we have $M = -a^3 = (-a)^3$, so M is again a cube in R . Thus in all cases $M \in R^m$. It follows that $[K(M^{1/m}) : K] = [K(a) : K] \leq 2$. If $m \geq 3$, then $x^m - M$ cannot be irreducible over K , for then $[K(a) : K] = m \geq 3$. By a well-known theorem (e.g. [9, Theorem 8.1.6]), it follows that either $m = 3$ and $M \in K^3$ or $m = 4$ and one of $M \in K^2$ or $M \in -4K^4$ holds. Note that in either of the cases for $m = 4$ we have $M^2 \in K^4$. However, we need not have $M \in K^4$ when $m = 4$, as evidenced by the example given in (10.1), where $K = \mathbb{Q}$, $R = \mathbb{Z}[i]$, and $a = (1 + i)$.

$m = 4$, μ -type (14): From Theorem 6.4, ϕ is Lattès of signature (2,4,4) with 0 and ∞ being points of signature 4, and hence satisfies case (2) of Theorem 1.3. Let ϕ have ramification structure (14) from Figure 3 with $\alpha_1 = \infty$ and $\alpha_2 = 0$. Then

$$\phi(x) = M \frac{f(x)^4}{x(x - \beta)^2 g(x)^4}, \quad \phi(x) - \beta = \frac{M}{x(x - \beta)^2 g(x)^4} [f(x)^4 - (\beta/M)x(x - \beta)^2 g(x)^4]$$

with $f(x)^4 - (\beta/M)x(x - \beta)^2 g(x)^4 = bh(x)^2$. Putting $x = 0$ or $x = \beta$ then gives $b \in K^2$, though yields no information about M . By the second remark following μ -type (13) (p. 34) we have $M^2 \in K^4$. Thus

$$\phi^2(x) \equiv M \frac{x(x - \beta)^2}{M} \frac{x^2(x - \beta)^4}{M^2 b^2} \equiv x^3(x - \beta)^2 \pmod{K(x)^4},$$

and a similar calculation gives $\phi^3(x) \equiv \phi(x) \pmod{K(x)^4}$.

$m = 3$, μ -type (4): From Theorem 6.4, ϕ is Lattès of signature (3,3,3) with 0 and ∞ in the post-critical set, and hence satisfies case (3) of Theorem 1.3. Replacing $\phi(x)$ by $1/\phi(1/x)$ if necessary, we may assume that $\alpha = \infty$ and $\beta = 0$ in entry (4) of Table 1. Then

$$\phi(x) = \gamma \frac{(x - \gamma)f(x)^3}{xg(x)^3}, \quad \phi(x) - \gamma = \frac{\gamma}{xg(x)^3} [(x - \gamma)f(x)^3 - xg(x)^3],$$

where $(x - \gamma)f(x)^3 - xg(x)^3 = bh(x)^3$ and the initial γ in $\phi(x)$ is because $\phi(\infty) = \gamma$. Putting $x = 0$ or $x = \gamma$ gives $b \in \gamma K^3$. Thus

$$\phi^2(x) \equiv \gamma \frac{\gamma^2}{x} \frac{x}{\gamma(x - \gamma)} \equiv \gamma^2(x - \gamma)^2 \pmod{K(x)^3},$$

and a similar calculation gives $\phi^3(x) \equiv x \pmod{K(x)^3}$.

$m = 3$, μ -type (2,1): From Theorem 6.4, ϕ is Lattès of signature (3,3,3) with 0 and ∞ in the post-critical set, and hence satisfies case (3) of Theorem 1.3. By the remark in Table 2, we have that ∞ is a simple fixed point for ϕ , while 0 and β lie in a two-cycle, mapping to one another with multiplicity one. Hence

$$\phi(x) = M \frac{(x - \beta)f(x)^3}{g(x)^3}, \quad \phi(x) - \beta = \frac{M}{g(x)^3} [(x - \beta)f(x)^3 - (\beta/M)g(x)^3]$$

with $(x - \beta)f(x)^3 - (\beta/M)g(x)^3 = bxh(x)^3$. Putting $x = 0$ gives $M \in K^3$ and putting $x = \beta$ gives $b \in K^3$. Thus $\phi^2(x) \equiv x \pmod{K(x)^3}$.

$m = 3$, μ -type (9): From Theorem 6.4, ϕ is Lattès of signature (3,3,3) with 0 and ∞ in the post-critical set, and hence satisfies case (3) of Theorem 1.3. We take $\alpha = \infty$ and $\beta_1 = 0$ in Table 2, and write β for β_2 . Hence

$$\phi(x) = M \frac{f(x)^3}{x(x - \beta)g(x)^3}, \quad \phi(x) - \beta = \frac{M}{x(x - \beta)g(x)^3} [f(x)^3 - (\beta/M)x(x - \beta)g(x)^3]$$

with $f(x)^3 - (\beta/M)x(x - \beta)g(x)^3 = bxh(x)^3$. Putting $x = 0$ or $x = \beta$ gives $b \in K^3$ and from the remark on p. 34 we have $M \in K^3$. It follows that $\phi^2(x) \equiv x^2(x - \beta)^2 \equiv \phi(x) \pmod{K(x)^3}$.

$m = 2$, μ -types (5a) and (5b): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3.

If ϕ has μ -type (5a), then taking $\alpha_1 = \infty$ and $\alpha_2 = 0$ ($\alpha = \infty$ and $\beta = 0$ in the notation of Figure 1) we have a four-cycle $\infty \mapsto \delta \mapsto \gamma \mapsto 0 \mapsto \infty$. Thus

$$\phi(x) = \delta \frac{(x - \gamma)f(x)^2}{xg(x)^2} \quad \phi(x) - \gamma = \frac{\delta b_1(x - \delta)h_1(x)^2}{xg(x)^2} \quad \phi(x) - \delta = \frac{\delta b_2 h_2(x)^2}{xg(x)^2},$$

where $(x - \gamma)f(x)^2 - (\gamma/\delta)xg(x)^2 = b_1(x - \delta)h_1(x)^2$ and $(x - \gamma)f(x)^2 - xg(x)^2 = b_2 h_2(x)^2$. Taking $x = 0$ in the first equation yields $b_1 \in \delta \gamma K^2$, and taking $x = 0$ in the second equation gives $b_2 \in -\gamma K^2$. Then

$$\phi^2(x) \equiv \delta \cdot \delta(x - \gamma) \cdot \delta b_1(x - \delta) \equiv \gamma(x - \gamma)(x - \delta) \pmod{K(x)^2}.$$

Similarly, we obtain $\phi^3(x) \equiv -\gamma\delta(x - \delta) \pmod{K(x)^2}$ and $\phi^4(x) \equiv x \pmod{K(x)^2}$.

If ϕ has μ -type (5b), we assume the four-cycle is of the form $\infty \mapsto \delta \mapsto 0 \mapsto \gamma \mapsto \infty$. The analysis in this case is quite similar to that of case (5a), though it leads to rather different-looking conclusions. We omit the details.

$m = 2$, μ -type (3,1): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3.

We take $\alpha_1 = \infty$ to be a fixed point of type (1) and $\alpha_2 = 0$ to be in a 3-cycle of type (3) along with β and γ . Without loss of generality, we take $\phi(\gamma) = \beta$ and $\phi(\beta) = 0$. This gives

$$\phi(x) = M \frac{(x - \beta)f(x)^2}{g(x)^2} \quad \phi(x) - \beta = \frac{Mb_1(x - \gamma)h_1(x)^2}{g(x)^2} \quad \phi(x) - \gamma = \frac{Mb_2 x h_2(x)^2}{g(x)^2},$$

where $(x - \beta)f(x)^2 - (\beta/M)g(x)^2 = b_1(x - \gamma)h_1(x)^2$ and $(x - \beta)f(x)^2 - (\gamma/M)g(x)^2 = b_2xh_2(x)^2$. Substituting $x = \gamma$ and $x = \beta$ into the first of these gives $\beta M(\gamma - \beta) \in K^2$ and $b_1\beta M(\gamma - \beta) \in K^2$, respectively. Hence $b_1 \in K^2$. Similar reasoning using the second equation gives $b_2 \in K^2$. Furthermore M must be a square in K (see Corollary 10.3 on p. 46). We now have

$$\phi(x) \in (x - \beta)K(x)^2, \quad \phi(x) - \beta \in (x - \gamma)K(x)^2, \quad \phi(x) - \gamma \in xK(x)^2.$$

From this it follows that $\phi^2(x) \equiv (x - \gamma) \pmod{K(x)^2}$ and $\phi^3(x) \equiv x \pmod{K(x)^2}$.

$m = 2$, μ -type (3): In the notation of Table 2, we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, giving a 3-cycle $C \mapsto \infty \mapsto 0 \mapsto C$ ($C \in \mathbb{C}^*$) of type (3) and it follows that

$$\phi(x) = B \frac{f(x)^2}{(x - C)g(x)^2}, \quad \phi(x) - C = \frac{B}{(x - C)g(x)^2} [f(x)^2 - (C/B)(x - C)g(x)^2]$$

with $\deg g \geq \deg f$ and

$$(8.5) \quad f(x)^2 - (C/B)(x - C)g(x)^2 = bxh(x)^2.$$

Note that $B, C \in K^*$ by Theorem 7.2. Putting $x = 0$ in (8.5) gives $-B \in K^2$ (note that $f(0), g(0) \neq 0$ since $\phi(0) \notin \{0, \infty\}$), and putting $x = C$ then gives $b \in CK^2$ ($f(C) \neq 0$ by assumption, whence $h(C) \neq 0$). Letting $D, E \in K$ satisfy $D^2 = -B$ and $b = CE^2$, we take $f_1(x) = Df(x) \in K[x]$ and $h_1(x) = DEh(x)$ to obtain $\phi(x) = -\frac{f_1(x)^2}{(x - C)g(x)^2}$ with $f_1(x)^2/D^2 - (C/B)(x - C)g(x)^2 = bxh_1(x)^2/(DE)^2$, i.e., $f_1(x)^2 + C(x - C) = Cxh_1(x)^2$. Writing $f(x)$ for $f_1(x)$ and $h(x)$ for $h_1(x)$ gives the form in (5a) of Theorem 1.3. Moreover,

$$\phi^2(x) \equiv B \cdot (\phi(x) - C) \equiv B \cdot Bbx(x - C) \equiv Cx(x - C) \pmod{K(x)^2},$$

A similar calculation gives $\phi^3(x) \equiv Cbx \equiv x \pmod{K(x)^2}$.

$m = 2$, μ -type (2,2): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3. We take $\alpha_1 = \infty$ to be in a 2-cycle of type (2) along with β_1 , and we take $\alpha_2 = 0$ to be in a similar 2-cycle along with β_2 . This gives

$$\phi(x) = \beta_1 \frac{(x - \beta_2)f(x)^2}{(x - \beta_1)g(x)^2} \quad \phi(x) - \beta_1 = \frac{b_1\beta_1h_1(x)^2}{(x - \beta_1)g(x)^2} \quad \phi(x) - \beta_2 = \frac{b_2\beta_1xh_2(x)^2}{(x - \beta_1)g(x)^2},$$

where $(x - \beta_2)f(x)^2 - (x - \beta_1)g(x)^2 = b_1h_1(x)^2$ and $(x - \beta_2)f(x)^2 - (\beta_2/\beta_1)(x - \beta_1)g(x)^2 = b_2xh_2(x)^2$. Taking $x = \beta_1$ in the first equation and then in the second equation, we obtain $b_1(\beta_1 - \beta_2) \in K^2$ and $b_2\beta_1(\beta_1 - \beta_2) \in K^2$, which gives $b_1b_2\beta_1 \in K^2$. It is now straightforward to check that $\phi^2(x) \equiv \beta_1b_1b_2x \equiv x \pmod{K(x)^2}$.

$m = 2$, μ -type (2,1): In the notation of Table 2 we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, so that ∞ is a fixed point of type (1) and 0 is in a 2-cycle of type (2), with C being the other point in this 2-cycle. We then have

$$\phi(x) = B \frac{(x - C)f(x)^2}{g(x)^2}, \quad \phi(x) - C = \frac{B}{g(x)^2} [(x - C)f(x)^2 - (C/B)g(x)^2]$$

with $(x - C)f(x)^2 - (C/B)g(x)^2 = bxh(x)^2$ and $B, C \in K^*$. Putting $x = 0$ gives $-B \in K^2$, and putting $x = C$ then gives $b \in K^2$, and one argues as in the μ -type (3) case, leading to the form in case 5(b) of Theorem 1.3. We then have $\phi^2(x) \equiv B \cdot BbxK(x)^2 \equiv x \pmod{K(x)^2}$.

$m = 2$, μ -type (12): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3. Assume that ∞ is the fixed point, with

preimages 0, β_1 , and β_2 of odd multiplicity. Then we have

$$\phi(x) = M \frac{f(x)^2}{x(x - \beta_1)(x - \beta_2)g(x)^2}, \quad \phi(x) - \beta_i = M \frac{b_i h_i(x)^2}{x(x - \beta_1)(x - \beta_2)g(x)^2},$$

where $f(x)^2 - (\beta_i/M)x(x - \beta_1)(x - \beta_2)g(x)^2 = b_i h_i(x)^2$ for $i = 1, 2$. Putting $x = 0$ gives $b_i \in K^2$, and one immediately obtains $\phi^2(x) \equiv x(x - \beta_1)(x - \beta_2) \pmod{K(x)^2}$ and $\phi^3(x) \equiv Mx(x - \beta_1)(x - \beta_2) \equiv \phi(x) \pmod{K(x)^2}$.

$m = 2$, μ -type (11): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3. If ϕ has μ -type (11a), let $\alpha_1 = \infty$ and $\alpha_2 = 0$, let β be the unique non-zero preimage of ∞ of ramification index one, and let γ be the unique finite preimage of 0 with ramification index one. We have

$$\phi(x) = C \frac{(x - \gamma)f(x)^2}{x(x - \beta)g(x)^2}, \quad \phi(x) - \gamma = \frac{Cb_1 h_1(x)^2}{x(x - \beta)g(x)^2}, \quad \phi(x) - \beta = \frac{Cb_2 h_2(x)^2}{x(x - \beta)g(x)^2},$$

where $(x - \gamma)f(x)^2 - (\gamma/C)x(x - \beta)g(x)^2 = b_1 h_1(x)^2$ and $(x - \gamma)f(x)^2 - (\beta/C)x(x - \beta)g(x)^2 = b_2 h_2(x)^2$. Putting $x = 0$ in the first equation gives $b_1 \in -\gamma K^2$, putting $x = \gamma$ gives $b_1 \in C(\beta - \gamma)K^2$ and putting $x = \beta$ gives $b_1 \in (\beta - \gamma)K^2$. Hence $C \in K^2$. Putting $x = 0$ in the second equation yields $b_2 \in -\gamma K^2$, and thus $b_1 b_2 \in K^2$. Now we obtain $\phi^2(x) \equiv b_1 b_2 x(x - \beta)(x - \gamma) \equiv \phi(x) \pmod{K(x)^2}$.

For type (11b), let ∞ and β be the points in the 2-cycle, and γ the unique finite preimage of β of odd multiplicity. Then

$$\phi(x) = \beta \frac{f(x)^2}{x(x - \beta)g(x)^2}, \quad \phi(x) - \gamma = \frac{\beta b_1 h_1(x)^2}{x(x - \beta)g(x)^2}, \quad \phi(x) - \beta = \frac{\beta b_2 (x - \gamma)h_2(x)^2}{x(x - \beta)g(x)^2},$$

where $f(x)^2 - (\gamma/\beta)x(x - \beta)g(x)^2 = b_1 h_1(x)^2$ and $f(x)^2 - x(x - \beta)g(x)^2 = b_2 (x - \gamma)h_2(x)^2$. Putting $x = 0$ in the first equation gives $b_1 \in K^2$, and putting $x = 0$ in the second equation gives $b_2 \in -\gamma K^2$. Hence $\phi^2(x) \equiv \beta b_2 (x - \gamma) \equiv -\beta \gamma (x - \gamma) \pmod{K(x)^2}$ and $\phi^3(x) \equiv -\gamma x(x - \beta) \pmod{K(x)^2}$. Also, $\phi^4(x) \equiv (x - \gamma) \pmod{K(x)^2}$ and $\phi^5(x) \equiv \beta x(x - \beta) \equiv \phi(x) \pmod{K(x)^2}$.

For type (11c), let ∞ and β be the points in the 2-cycle, and γ the unique preimage of ∞ of odd multiplicity not contained in the 2-cycle (i.e. not equal to β). Then

$$\phi(x) = \beta \frac{f(x)^2}{(x - \beta)(x - \gamma)g(x)^2}, \quad \phi(x) - \gamma = \frac{\beta b_1 h_1(x)^2}{(x - \beta)(x - \gamma)g(x)^2}, \quad \phi(x) - \beta = \frac{\beta b_2 x h_2(x)^2}{(x - \beta)(x - \gamma)g(x)^2},$$

where $f(x)^2 - (\gamma/\beta)(x - \beta)(x - \gamma)g(x)^2 = b_1 h_1(x)^2$ and $f(x)^2 - (x - \beta)(x - \gamma)g(x)^2 = b_2 x h_2(x)^2$. Putting $x = \beta$ in the first equation gives $b_1 \in K^2$, and putting $x = 0$ and $x = \beta$ in the second equation give respectively $\beta \gamma \in K^2$ and $b_2 \in \beta K^2$. Hence $\phi^2(x) \in xK(x)^2$.

$m = 2$, μ -type (10): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3. For μ -type (10a) we have $\phi(0) = \infty$, and thus

$$\phi(x) = M \frac{(x - \gamma_1)(x - \gamma_2)f(x)^2}{xg(x)^2}, \quad \phi(x) - \gamma_1 = \frac{Mb_1 h_1(x)^2}{xg(x)^2}, \quad \phi(x) - \gamma_2 = \frac{Mb_2 h_2(x)^2}{xg(x)^2},$$

where $(x - \gamma_1)(x - \gamma_2)f(x)^2 - (\gamma_i/M)xg(x)^2 = b_i h_i(x)^2$ for $i = 1, 2$. Putting $x = 0$ yields $b_i \in \gamma_1 \gamma_2 K^2$, and putting $x = \gamma_1$ gives $b_i \in -M\gamma_i \gamma_1 K^2$. Thus $b_2 \in \gamma_1 \gamma_2 K^2$ and $b_2 \in -M\gamma_1 \gamma_2 K^2$, showing that $-M \in K^2$. But $b_1 \in -MK^2$, so $b_1 \in K^2$, and it easily follows that $b_2 \in K^2$. Then $\phi^2(x) \equiv x(x - \gamma_1)(x - \gamma_2) \pmod{K(x)^2}$ and $\phi^3(x) \equiv Mx(x - \gamma_1)(x - \gamma_2) \equiv \phi(x) \pmod{K(x)^2}$.

For μ -type (10b) we have $\phi(\beta) = \infty$ with 0 and γ the pre-images of β occurring to odd multiplicity. Thus

$$\phi(x) = M \frac{f(x)^2}{(x - \beta)g(x)^2}, \quad \phi(x) - \beta = \frac{Mb_1x(x - \gamma)h_1(x)^2}{(x - \beta)g(x)^2}, \quad \phi(x) - \gamma = \frac{Mb_2h_2(x)^2}{(x - \beta)g(x)^2},$$

where $f(x)^2 - (\beta/M)(x - \beta)g(x)^2 = b_1x(x - \gamma)h_1(x)^2$ and $f(x)^2 - (\gamma/M)(x - \beta)g(x)^2 = b_2h_2(x)^2$. Putting $x = 0$ in the first equation yields $-M \in K^2$, while putting $x = \beta$ gives $b_1\beta(\beta - \gamma) \in K^2$ and putting $x = \gamma$ and using $-M \in K^2$ gives $\beta(\beta - \gamma) \in K^2$. Therefore $b_1 \in K^2$. Putting $x = \beta$ in the second equation yields $b_2 \in K^2$. Then $\phi^2(x) \equiv M \cdot Mx(x - \beta)(x - \gamma) \equiv x(x - \beta)(x - \gamma) \pmod{K(x)^2}$, $\phi^3(x) \equiv M(x - \beta) \cdot Mx(x - \beta)(x - \gamma) \cdot M(x - \beta) \equiv Mx(x - \beta)(x - \gamma) \pmod{K(x)^2}$, and $\phi^4(x) \equiv \phi^2(x) \pmod{K(x)^2}$.

μ -type (8): In the notation of Table 2 we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, so that ∞ and C are the preimages of 0 having odd multiplicity. Thus

$$\phi(x) = B \frac{(x - C)f(x)^2}{g(x)^2}, \quad \phi(x) - C = \frac{B}{g(x)^2} [(x - C)f(x)^2 - (C/B)g(x)^2]$$

with $\deg g(x) \geq 1 + \deg f(x)$, $(x - C)f(x)^2 - (C/B)g(x)^2 = bh(x)^2$, and $B, C \in K^*$. Putting $x = C$ gives $b \in -BCK^2$, leading to the form in case 5(c) of Theorem 1.3. Note that in contrast to cases 5(a) and 5(b), the image of B in K^*/K^{*2} is not determined. An easy calculation shows $\phi^2(x) \equiv B \cdot Bb \equiv -BC \pmod{K(x)^2}$, and hence $\phi^3(x) \equiv \phi^2(x) \pmod{K(x)^2}$.

$m = 2$, μ -type (7,7): From Theorem 6.4, ϕ is Lattès of signature (2,2,2,2) with 0 and ∞ in the post-critical set, and hence satisfies case (4) of Theorem 1.3. We assume that ∞ is a fixed point of type (7), with β_1 its unique preimage of multiplicity one, and similarly for 0 and β_2 . We have

$$\phi(x) = M \frac{x(x - \beta_2)f(x)^2}{(x - \beta_1)g(x)^2}, \quad \phi(x) - \beta_1 = \frac{Mb_1h_1(x)^2}{(x - \beta_1)g(x)^2}, \quad \phi(x) - \beta_2 = \frac{Mb_2h_2(x)^2}{(x - \beta_1)g(x)^2},$$

where $x(x - \beta_2)f(x)^2 - (\beta_i/M)(x - \beta_1)g(x)^2 = b_ih_i(x)^2$ for $i = 1, 2$. Putting $x = 0$ yields $b_1 \in MK^2$ ($i = 1$) and $b_2 \in \beta_1\beta_2MK^2$ ($i = 2$). Putting $x = \beta_1$ yields $b_i \in \beta_1(\beta_1 - \beta_2)K^2$, and putting $x = \beta_2$ yields $\beta_i(\beta_1 - \beta_2) \in Mb_iK^2$. Using $b_1 \in \beta_1(\beta_1 - \beta_2)K^2$ and $\beta_1(\beta_1 - \beta_2) \in Mb_1K^2$ yields $M \in K^2$, and it quickly follows that $b_1 \in K^2$ and $b_2 \in K^2$. We now have $\phi^2(x) \equiv x(x - \beta_1)(x - \beta_2) \equiv \phi(x) \pmod{K(x)^2}$.

μ -type (7,6): In the notation of Table 2 we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, so that ∞ is a point of type (6) and 0 is a fixed point of type (7) with unique non-zero preimage C of odd multiplicity. Thus

$$\phi(x) = B \frac{x(x - C)f(x)^2}{g(x)^2}, \quad \phi(x) - C = \frac{B}{g(x)^2} [x(x - C)f(x)^2 - (C/B)g(x)^2]$$

with $x(x - C)f(x)^2 - (C/B)g(x)^2 = bh(x)^2$ and $B, C \in K^*$. Putting $x = 0$ or $x = C$ gives $b \in -BCK^2$, leading to the form in 5(d) of Theorem 1.3. We also have $\phi^2(x) \equiv B \cdot Bx(x - C) \cdot Bb \equiv -Cx(x - C) \pmod{K(x)^2}$, and $\phi^3(x) \equiv Bx(x - C) \equiv \phi(x) \pmod{K(x)^2}$. \square

9. PROOF OF THEOREM 1.1

Proof of Theorem 1.1. We first argue that we can reduce to the case where $\lambda(x) = x^m$. Indeed, because λ has two totally ramified fixed points in $\mathbb{P}^1(K)$, there is some Möbius transformation $\mu \in K(x)$ with $(\mu \circ \lambda \circ \mu^{-1})(x) = x^m$. Now for $a, b \in \mathbb{P}^1(K)$, we have $(\mu \circ \phi \circ \mu^{-1})(\mu(a)) = b^m$ (we put $\infty^m = \infty$) if and only if $\mu(\phi(a)) = b^m$, i.e. $\phi(a) = \mu^{-1}(b^m) = \lambda(\mu^{-1}(b))$. It follows that

$$(9.1) \quad (\mu \circ \phi \circ \mu^{-1})(\mu(a)) \in \mathbb{P}^1(K)^m \text{ if and only if } \phi(a) \in \lambda(\mathbb{P}^1(K)).$$

Hence to prove the theorem, it suffices to consider the set $O_\phi(a) \cap \mathbb{P}^1(K)^m$ for any $\phi \in K(x)$ and $a \in \mathbb{P}^1(K)$. Moreover, taking $\lambda(x) = x^m$ and $\mu(x) = 1/x$ in (9.1) (see also (6.2)), we have that it suffices to consider the set $O_\phi(a) \cap \mathbb{P}^1(K)^m$ for a single element ϕ of each μ -conjugacy class.

Suppose that $a \in \mathbb{P}^1(K)$ and $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite, and let C_n be the curve given by $\phi^n(x) = y^m$. As in the paragraph following Conjecture 1.2, $C_n(K)$ is infinite for all $n \geq 1$, and by Faltings' Theorem the genus of C_n must be at most one for all $n \geq 1$. From Corollary 2.3, we then have that $A = \{0, \infty\}$ is a set of m -branch abundant points for ϕ . By Theorem 1.4, we have

$$(9.2) \quad \phi^r(x) = \phi^s(x)(\psi(x))^m \quad \text{for some } r > s \geq 0 \text{ and } \psi(x) \in K(x).$$

In particular, (9.2) implies that for all $\ell \geq 0$,

$$(9.3) \quad \phi^{\ell(r-s)+i}(x) \equiv \phi^i(x) \pmod{K(x)^{*m}} \quad \text{for all } i = s, \dots, r-1.$$

For $n \geq 0$, put

$$(9.4) \quad k_n = \begin{cases} n & \text{if } n < s \\ i & \text{if } n = \ell(r-s) + i \text{ for } \ell \geq 0 \text{ and } s \leq i \leq r-1 \end{cases}$$

From (9.2) and (9.3) we can write $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ as

$$(9.5) \quad \{n \geq 0 : \phi^{k_n}(a) \in K^m\} \cup \{n \geq 0 : \phi^n(a) \in \{0, \infty\}\}.$$

Because $O_\phi(a)$ is infinite, each of 0 and ∞ can appear at most once in the sequence $(\phi^n(a) : n \geq 0)$. It follows from (9.5) that $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a finite union of arithmetic progressions. Moreover the modulus of each arithmetic progression is bounded by $r-s$, and from Theorem 1.4 we have $r-s \leq m$ for $m \geq 3$ and $r-s \leq 4$ for $m = 2$. Thus to prove Theorem 1.1 it remains only to show that the set in (9.5) is in fact the union of at most three arithmetic progressions.

If $\phi(x) = cx^j(\psi(x))^m$, we show in Proposition 9.1 that $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a single (possibly empty) arithmetic progression. We thus restrict our attention to the non-trivial μ -types in Table 2. We make a slightly different partition from the one given in (9.5): write $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = I \cup F$, where $I = \{n \geq s : \phi^{k_n}(a) \in K^m\}$, and

$$F = \{0 \leq n < s : \phi^{k_n}(a) \in K^m\} \cup \{n \geq 0 : \phi^n(a) \in \{0, \infty\}\}.$$

It follows from (8.2) and (9.4) that we can write I as a single infinite arithmetic progression if $r-s \leq 2$ or a union of at most two infinite arithmetic progressions if $3 \leq (r-s) \leq 4$.

Again from Table 4, we may take $s \in \{0, 1\}$ unless $m = 2$ and ϕ has μ -type (10b) or (8), in which case we may take $s = 2$. Suppose first that $O_\phi(a) \cap \{0, \infty\} = \emptyset$. Then $\#F \leq 2$, with equality only in the case of μ -type (10b) or (8). But for both of these I can be written as a single arithmetic progression, meaning that $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most three arithmetic progressions.

Suppose now that $O_\phi(a) \cap \{0, \infty\} \neq \emptyset$. Because $A = \{0, \infty\}$ is a set of m -branch abundant points for ϕ , it follows from Table 2 that ϕ has μ -type (8) or (7,6), since otherwise both 0 and ∞ have finite forward orbits. For both of these μ -types, precisely one of 0, ∞ has infinite forward orbit. For μ -type (8) we have $I = \mathbb{Z} \setminus \{0, 1\}$ (recall that $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite by assumption), and it follows that $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most two arithmetic progressions. For μ -type (7,6) we have $s = 1$ and so $\#F \leq 2$; but I can be written as at most one arithmetic progression, and so we are done. \square

Proposition 9.1. *Let K be a number field and suppose that $\phi = cx^j\psi(x)^m$ for some $0 \leq j \leq m-1$, $m \geq 2$, $c \in K \setminus \{0\}$, and $\psi \in K(x)$. Let t be the minimal positive integer such that $c^t \in K^m$, and suppose that $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite for some $a \in \mathbb{P}^1(K)$. Then $\gcd(t, j) = 1$ and we have*

$$\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = \ell + M\mathbb{N},$$

where ℓ is a non-negative integer and

$$M = \begin{cases} t & \text{if } j = 1 \\ \text{ord}_{t(j-1)}(j) & \text{otherwise,} \end{cases}$$

where $\text{ord}_{t(j-1)}(j)$ is the order of j in the group $(\mathbb{Z}/t(j-1)\mathbb{Z})^*$. In all cases, $M \leq m$.

Proof. Suppose first that $j = 0$, so that $\phi(x) = c\psi(x)^m$. If $t > 1$ then $c \notin K^m$, and hence we have $\phi(a) \notin K^m$ for all $a \in \mathbb{P}^1(K)$ with $\phi(a) \neq 0, \infty$. This forces $O_\phi(a) \cap \mathbb{P}^1(K)^m$ to be finite, a contradiction. Therefore $t = 1$ and $c \in K^m$, whence $\phi(a) \in K^m$ for all $a \in \mathbb{P}^1(K)$, implying that $\{n \geq 0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = \ell + M\mathbb{N}$ with $M = 1$ and $\ell = 0$ (if $a \in K^m$) or $\ell = 1$ (otherwise). This proves the proposition in this case.

Now suppose that $j > 0$. Because $0 < j < m$ and the order of any zero or pole of $\psi(x)^m$ is divisible by m , we must have $\phi(0) \in \{0, \infty\}$ and $\phi(\infty) \in \{0, \infty\}$. The infinitude of $O_\phi(a)$ then implies that $O_\phi(a) \cap \{0, \infty\} = \emptyset$. Let ℓ be the minimal non-negative integer with $\phi^\ell(a) \in \mathbb{P}^1(K)^m$, and because $\phi^\ell(a) \neq \infty$ we may write $\phi^\ell(a) = b^m$ for some $b \in K$. For any $r \geq 1$, we have (cf. (8.1))

$$\phi^{\ell+r}(a) = c^{1+j+\dots+j^{r-1}}(b^m)^{j^r}(\psi_r(b^m))^m,$$

for some $\psi_r(x) \in K(x)$. Because $\phi^{\ell+r}(a) \neq 0, \infty$ we have $\phi^{\ell+r}(a) \in K^*$, and hence $\phi^{\ell+r}(a) \in K^m$ if and only if $c^{1+j+\dots+j^{r-1}} \in K^{*m}$. Note that t is the order of c in the group K^*/K^{*m} , and hence we have $c^i \in K^{*m}$ if and only if $t \mid i$. We thus wish to find all u such that

$$(9.6) \quad 1 + j + \dots + j^{u-1} \equiv 0 \pmod{t}.$$

If $g := \gcd(t, j) \neq 1$, then the left-hand side of (9.6) is 1 modulo g , and hence cannot be 0 modulo t . Thus no u exists satisfying (9.6), and we conclude that $O_\phi(a) \cap \mathbb{P}^1(K)^m$ consists of the single element $\{\phi^\ell(a)\}$, a contradiction. Therefore $\gcd(t, j) = 1$. If $j = 1$, then (9.6) holds if and only if u is a multiple of t . If $j \neq 1$, then note that j is relatively prime to both $j-1$ and t , and let M be the order of j in $(\mathbb{Z}/t(j-1)\mathbb{Z})^*$. Then (9.6) is equivalent to $(j^u - 1)/(j - 1) \equiv 0 \pmod{t}$, i.e., $j^u - 1 \equiv 0 \pmod{t(j-1)}$, which holds if and only if u is a multiple of M . \square

Remark. Proposition 9.1 shows that the bound $M \leq m$ for $m \geq 3$ from Theorem 1.1 is attained regardless of the choice of K : let $c \in K$ with $c \notin K^{*p}$ for all primes $p \mid m$, and let $\phi(x) = cx(x+1)^m$. Then $t = m$ in the statement of Proposition 9.1, and we have $O_\phi(1) \cap \mathbb{P}^1(K)^m = \{\phi^{km}(1) : k \geq 0\}$. When $m = 2$, arithmetic progressions of modulus 3 are possible over any field K (see p. 48). There exist number fields K and maps $\phi(x)$ possessing orbits with $M = 4$ (see the map in (10.6)). However, it is not clear whether such maps may be defined over a given number field K , e.g. $K = \mathbb{Q}$. See the discussion on p. 47.

10. LATTÈS MAPS AND EXAMPLES

In this section we construct many examples of non-trivial maps $\phi \in \mathbb{C}(x)$ of degree at least 2 and with a set A of two distinct m -branch abundant points (necessarily with $2 \leq m \leq 4$, by Lemma 6.3). In particular, we give a complete classification of the post-critical structures of Lattès maps, and show that Lattès maps realize all of the non-trivial μ -types in Table 2. We give further examples

where $A = \{0, \infty\}$, ϕ is defined over a number field K , and $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite for some $a \in \mathbb{P}^1(K)$. Some of these examples show that the bounds for M and the number of arithmetic progressions given in Theorem 1.1 are sharp, or nearly sharp.

10.1. Lattès maps. Following [11], we define a Lattès map ϕ to be given by a linear map $L(t) = at + b$ acting on a complex torus \mathbb{C}/Λ and a finite-to-one holomorphic map $\Theta : \mathbb{C}/\Lambda \rightarrow \mathbb{P}^1(\mathbb{C})$. We then obtain $\phi : \mathbb{P}^1(\mathbb{C}) \rightarrow \mathbb{P}^1(\mathbb{C})$ as the unique map satisfying $\phi \circ \Theta = \Theta \circ L$. Moreover, a, b, Λ , and Θ all must satisfy various properties; for instance $a\Lambda \subset \Lambda$ (whence $a \in \Lambda$), $\zeta_n\Lambda = \Lambda$, and $(1 - \zeta_n)b \in \Lambda$, where ζ_n is a primitive n th root of unity [11, Theorem 5.1]. Moreover, up to conformal conjugacy Θ may be taken to be the natural projection $\mathbb{C}/\Lambda \rightarrow (\mathbb{C}/\Lambda)/G_n$, where G_n is the group of n th roots of unity ($n \in \{2, 3, 4, 6\}$) acting on \mathbb{C}/Λ by rotation about a base point, and L commutes with the action of a generator of G_n ([11, Theorem 3.1]). Since L is unramified, it follows that the post-critical set of ϕ consists of the set V_Θ of all critical values of Θ ([11, Lemma 3.4]), and thus the action of ϕ on its post-critical set is given by the action of L on V_Θ . We now enumerate the possibilities for this action.

10.2. Lattès maps of signature (2,3,6). Lattès maps of this signature must descend from elliptic curves with complex multiplication (the rationale is similar to that in Section 10.3). Let $\delta_2, \delta_3, \delta_6$ be the points of signature 2, 3, and 6, respectively. By the definition of signature (see Theorem 6.1) we have $\phi(\delta_6) = \delta_6$ with multiplicity 1, $\phi(\delta_3) = \delta_3$ with multiplicity 1 or $\phi(\delta_3) = \delta_6$ with multiplicity 2, and $\phi(\delta_2) = \delta_2$ with multiplicity 1 or $\phi(\delta_2) = \delta_6$ with multiplicity 3. Hence the set of 3-branch abundant points for ϕ is $A = \{\delta_6, \delta_3\}$, and ϕ must have μ -type (1,1) or (7); in either case ϕ is trivial with respect to A . The set of 2-branch abundant points for ϕ is $\{\delta_6, \delta_2\}$, and ϕ must again have μ -type (1,1) or (7); in either case ϕ is trivial with respect to A . Because all maps of this signature are trivial for the purposes of this paper, we limit ourselves to this elementary analysis.

10.3. Lattès maps of signature (2,4,4). In the notation of Section 10.1 this requires $n = 4$ ([11, Remark 4.6]), and so we must choose Λ so that it admits a rotation of order 4; note that this implies that \mathbb{C}/Λ has complex multiplication. In fact, we must have $\Lambda = \mathbb{Z}[i]$, which admits the rotation $\omega_4 : z \mapsto iz$. The set of critical values V_Θ of Θ then is given by those ω_4 -orbits in \mathbb{C}/Λ that contain either one or two elements. This gives

$$V_\Theta = \{[1/2], [0], [1/2 + i/2]\},$$

where $[t]$ denotes the orbit of $t \in \mathbb{C}/\Lambda$ under $G_4 = \langle \omega_4 \rangle$. Note that $[0]$ and $[1/2 + i/2]$ both have a single element, and thus correspond to points of signature 4, while $[1/2] = \{1/2, i/2\}$ and so corresponds to a point of signature 2. The stipulation $(1 - i)b \in \Lambda$ implies that $b \equiv 0$ or $b \equiv 1/2 + i/2$ modulo Λ . Moreover, the action of L on V_Θ is determined by the (additive) equivalence class of b modulo Λ and a modulo 2Λ , since multiplication by an element of 2Λ sends V_Θ to $[0]$.

If $a \equiv 1 + i \pmod{2\Lambda}$, then $[b]$ is a fixed point for L , the point $[b + 1/2 + i/2]$ (the other point in V_Θ of signature 4) maps to $[b]$, and the point of signature 2 maps to $[b + 1/2 + i/2]$.

If $a \equiv 0 \pmod{2\Lambda}$, then L maps V_Θ to the fixed point $[b]$.

If $a \equiv 1 \pmod{2\Lambda}$ or $a \equiv i \pmod{2\Lambda}$, then $t \mapsto at$ acts as the identity on V_Θ , and hence either L acts as the identity on V_Θ (if $b \equiv 0 \pmod{\Lambda}$) or L fixes $[1/2]$ and interchanges the other two points of V_Θ (if $b \equiv 1/2 + i/2 \pmod{\Lambda}$).

Suppose that $m = 4$, and note that the set of 4-branch abundant points for ϕ is $A = \{[0], [1/2 + i/2]\}$. If $a \equiv 1 + i \pmod{2\Lambda}$, then ϕ has μ -type (13). If $a \equiv 0 \pmod{2\Lambda}$ then ϕ has μ -type (14). If $a \equiv 1 \pmod{2\Lambda}$ or $a \equiv i \pmod{2\Lambda}$, then ϕ has μ -type (1,1) (when $b \equiv 0 \pmod{\Lambda}$) or (2) (when $b \equiv 1/2 + i/2 \pmod{\Lambda}$); in both of these cases ϕ is trivial with respect to A .

When $m = 2$, then ϕ has three 2-branch abundant points, namely those in V_Θ . Depending on the choice of two-element subset $A \subset V_\Theta$, ϕ has μ -type (6,6), (7,6), or (7) if $a \equiv 1 + i$ or $0 \pmod{2\Lambda}$, and ϕ has μ -type (1,1), (2,1), or (2) if $a \equiv 1$ or $i \pmod{2\Lambda}$. Thus μ is either trivial with respect to $\{0, \infty\}$ or has μ -type (7,6) or (2,1). We give further examples of these kinds in Section 10.7, and postpone their discussion for now.

Let us return to the case of $m = 4$, where K is a number field; we construct some maps $\phi \in K(x)$ with $A = \{0, \infty\}$. Let $a = 1 + i$ and $b = 0$, so that ϕ has degree $N(1 + i) = 2$, and assume that $[0] = \infty$, $[1/2 + i/2] = 0$, and $[1/2] = B \in K$. From [11, Corollary 3.9] the fixed point of ϕ at ∞ has multiplier $(1 + i)^4 = -4$. Hence

$$(10.1) \quad \phi(x) = -\frac{(x - B)^2}{4x}.$$

One can check directly that the other critical point of ϕ besides B is $-B$, and moreover $\phi(-B) = B$. Thus every map of the form (10.1) has μ -type (13). Note that conjugating ϕ by the scaling $x \mapsto cx$ yields the map $-\frac{(x - cB)^2}{4x}$, and it follows that maps of the form (10.1) are conjugate to each other. Let $B = -3$ and note that the curve $y^4 = \phi(x)$ has the rational point $(-1, 1)$, implying by Table 4 that $\phi^{2j+1}(-1)$ is a fourth power in \mathbb{Q} for all $j \geq 0$. Indeed, we have

$$O_\phi(-1) = \left\{ -1, 1, -4, \left(\frac{1}{2}\right)^4, -\frac{1}{4}\left(\frac{7}{2}\right)^4, \left(\frac{47}{28}\right)^4, \dots \right\}$$

One can show that $O_\phi(-1)$ is in fact infinite (one method is to find the periodic points of ϕ modulo 5 and 7 and conclude that ∞ is the only pre-periodic point of ϕ in $\mathbb{P}^1(\mathbb{Q})$; cf. [14, Section 2.6].) We remark that $\phi^2(-1) = -4$ is not a fourth power in \mathbb{Q} , and thus from Table 4 we have that $\phi^{2j+2}(-1)$ is not a fourth power in \mathbb{Q} , for all $j \geq 0$. On the other hand, $\phi^2(-1)$ is a fourth power in $\mathbb{Q}(i)$, and thus every element of $O_\phi(-1)$ is a fourth power in $\mathbb{Q}(i)$.

Letting ϕ be as in (10.1), we have

$$\phi^2(x) = \frac{(x + B)^4}{16x(x - B)^2},$$

which descends from the linear map $L(t) = (1 + i)^2 t = 2it$, and hence satisfies $a \equiv 0 \pmod{2\Lambda}$, and so has μ -type (14).

10.4. Lattès maps of signature (3,3,3). In the notation of Section 10.1 this requires $n = 3$ ([11, Remark 4.6]), and so we must choose Λ so that it admits a rotation of order 3. It follows that $\Lambda = \mathbb{Z}[\zeta_6]$, where ζ_6 is a primitive 6th roots of unity; this lattice admits the rotation $\omega_3 : z \mapsto \zeta_6^2 z$ of order 3. The set of critical values V_Θ of Θ then is given by those ω_3 -orbits in \mathbb{C}/Λ that contain a single element, and hence are fixed. A straightforward calculation gives

$$V_\Theta = \{[0], [(1 + \zeta_6)/3], [2(1 + \zeta_6)/3]\},$$

where $[t]$ denotes the orbit of $t \in \mathbb{C}/\Lambda$ under $G_3 = \langle \omega_3 \rangle$. We also use the notation V_Θ to refer to the subset $\{0, (1 + \zeta_6)/3, 2(1 + \zeta_6)/3\}$ of \mathbb{C}/Λ , which we note is a subgroup of \mathbb{C}/Λ . Now because $(1 - \zeta_6^2)b \in \Lambda$, we have that b is equivalent to $j(1 + \zeta_6)/3$ modulo Λ , where $j \in \{0, 1, 2\}$. Moreover, the action of L on V_Θ is determined by the equivalence class of b modulo Λ and the equivalence class of a modulo $(1 + \zeta_6)\Lambda$, since $z \mapsto (1 + \zeta_6)z$ is the zero map on V_Θ . Note that $a \equiv 0, 1$, or $2 \pmod{(1 + \zeta_6)\Lambda}$.

The maps $t \mapsto at$ and $t \mapsto (a - 1)t$ induce homomorphisms $(a), (a - 1) : V_\Theta \rightarrow V_\Theta$. It is straightforward to check that (a) is the zero map if and only if $a \equiv 0 \pmod{(1 + \zeta_6)\Lambda}$, from which it follows that $(a - 1)$ is the zero map if and only if $a \equiv 1 \pmod{(1 + \zeta_6)\Lambda}$.

If $a \equiv 2 \pmod{(1 + \zeta_6)\Lambda}$, then both (a) and $(a - 1)$ are isomorphisms on V_Θ , and thus L acts on V_Θ one-to-one and with a unique fixed point. Therefore L acts on V_Θ with one two-cycle and one fixed point.

If $a \equiv 1 \pmod{(1 + \zeta_6)\Lambda}$, then (a) is an isomorphism and $(a - 1)$ is the zero map on V_Θ . Thus L acts on V_Θ one-to-one and with three fixed points (if $b \in \text{im}(a - 1)$, i.e. if $b = 0$) and no fixed points otherwise. In the former case, L is the identity on V_Θ , while in the latter L acts on V_Θ as a three-cycle.

If $a \equiv 0 \pmod{(1 + \zeta_6)\Lambda}$, then L maps V_Θ to the fixed point $[b]$.

In all cases, V_Θ is the set of 3-branch abundant points for ϕ ; let $A \subset V_\Theta$ have two elements. If $a \equiv 2 \pmod{(1 + \zeta_6)\Lambda}$, then ϕ has μ -type (2) if the points of A lie in the 2-cycle and μ -type (2, 1) otherwise. If $a \equiv 1 \pmod{(1 + \zeta_6)\Lambda}$, then ϕ has μ -type (1,1) if $b = 0$ and μ -type (4) otherwise. If $a \equiv 0 \pmod{(1 + \zeta_6)\Lambda}$, then ϕ has μ -type (6,6) if neither element of A is fixed by ϕ , and μ -type (9) otherwise.

We now construct some examples with $A = \{0, \infty\}$. Taking $a = 2$ and $b = 0$ gives a map of μ -type (2,1), and we can find a representation for such a map as follows. We may decompose Θ as the composition of the Weierstrass \mathfrak{p} -function and a finite morphism $\pi : E \rightarrow \mathbb{P}^1$, where E is an elliptic curve in Weierstrass form isomorphic over \mathbb{C} to $\mathbb{C}/\mathbb{Z}[\zeta_6]$. Hence we may take E to be given by $y^2 = x^3 + B^2$ with $B \in \mathbb{C}$ (our reasons for writing B^2 will become clear in a moment). Moreover, we may take $\pi(x, y) = y$ [14, Proposition 6.37]. Using the standard formula for the doubling map on an elliptic curve (see e.g. [14, Example 6.66]), we obtain $\phi_0(x) = \frac{x(x^3 - 8B^2)}{4(x^3 + B^2)}$. To write the image of the y -coordinate of this map as a function of y , we calculate $\phi_0(x)^3 + B^2$, use the relation $y^2 = x^3 + B^2$, and then take a square root. This yields the function $\phi_1(y) = (y^4 + 18B^2y^2 - 27B^4)/8y^3$. The critical points of ϕ_1 are $0, \pm 3B$, each of multiplicity 3. Their images are ∞ and $\pm B$, and ∞ is a fixed point while $\pm B$ lie in a 2-cycle. In order to make points of signature 3 lie at both 0 and ∞ , we conjugate by $y \mapsto y + B$ and to match our usual notation we replace the variable y by x to get

$$(10.2) \quad \phi(x) = \frac{(x - 2B)(x + 2B)^3}{8(x - B)^3}.$$

This map has ramification type (2,1) with fixed point ∞ and 2-cycle $\{0, 2B\}$. Because $\phi^2(x) \equiv x \pmod{K(x)^{*3}}$, we may construct an orbit containing infinitely many distinct cubes by taking a non-preperiodic a that is also a cube in K . If $a - 2B$ is also a cube in K , then every element of $O_\phi(a)$ is a cube in K ; otherwise only terms of the form $\phi^{2j}(x_0)$ will be cubes. For example, taking $B = 1$ and $a = -1$ yields an infinite orbit where the cubes occur at precisely the even indices.

We can also find an example of a map of μ -type (4) by piggybacking on the work just done. Pre-composing the map in (10.2) with the Möbius transformation $x \mapsto 4B^2/x$ preserves both the multiplicity of the three critical points and the fact that the post-critical set consists of the non-critical points $\{0, 2B, \infty\}$. However, now these three points are in a 3-cycle $0 \mapsto \infty \mapsto 2B \mapsto 0$, and hence the resulting map has ramification structure (4):

$$(10.3) \quad \phi(x) = \frac{2B(x - 2B)(x + 2B)^3}{x(x - 4B)^3}.$$

The only element of Λ that has norm 4 and is congruent to 1 $\pmod{(1 + \zeta_6)\Lambda}$ is $2\zeta_6$, and hence ϕ descends from a linear map of the form $L(t) = (2\zeta_6)t + b$ with $b \in \{(1 + \zeta_6)/3, 2(1 + \zeta_6)/3\}$. It is now simple to construct a rational orbit where, say, cubes occur at terms of the form $\phi^{3k+2}(a)$. For

instance, take $B = 1$ in (10.3) and set $a = 6$. Then

$$O_\phi(6) = \left\{ 6, \frac{4}{3} \cdot 4^3, \left(\frac{655}{488} \right)^3, 6 \left(-\frac{129900299507}{120418942015} \right)^3, \dots \right\}$$

which one can check is infinite. Note that for any map ϕ of μ -type (4), we have from Table 4 that $\phi(x)\phi^2(x)\phi^3(x) \in K(x)^{*3}$, and hence if $\phi^i(a) \in K^3$ for two $i \in \{1, 2, 3\}$, then the same conclusion holds for all three. Hence one cannot construct an orbit where the cubes occur precisely at the union of two infinite arithmetic progressions. On the other hand, one can do this with squares; see p. 48.

To construct examples of μ -type (9), the smallest-norm value of a that suffices is $1 + \zeta_6$, which gives rise to a map ϕ of degree 3. However, in this case ϕ is only defined over number fields containing ζ_6 , since by [11, Corollary 3.9] its multiplier at the fixed point ∞ is $(1 + \zeta_6)^3 = 6\zeta_6 - 3$. Taking $a = 3$ and $b = 0$ gives rise to the following Lattès map, which we calculate by finding the y -coordinate of the tripling map on the curve $E : y^2 = x^3 + B^2$:

$$\phi_0(y) = \frac{y(y^2 - 9B^2)(y^6 + 225B^2y^4 - 405B^4y^2 + 243B^6)}{27(y^2 - B)(y^2 + 3B^2)^3}.$$

The points of signature 3 for ϕ_0 are ∞ and $\pm B$, and to ensure 0 is also a point of signature 3, we conjugate by $y \mapsto y + B$ and replace y by x to get

$$(10.4) \quad \phi(x) = \frac{(x^3 + 6Bx^2 - 24B^2x + 8B^3)^3}{27x(x - 2B)(x^2 - 2Bx + 4B^2)^3}.$$

The points of signature 3 for ϕ are ∞ , 0, and $2B$. Note that for $a \in K$, $\phi(a) \in K^3$ is equivalent to $a(a - 2B) \in K^3$, i.e. a is the x -coordinate of a K -rational point on the elliptic curve $E : y^3 = x(x - 2B)$. From Table 4, we have $\phi(a) \in K^3$ if and only if $\phi^n(a) \in K^3$ for all $n \geq 1$, i.e., $\phi(\phi^{n-1}(a)) \in K^3$ for all $n \geq 1$. It follows that there is a K -orbit containing infinitely many distinct cubes if and only if $E(K)$ has positive rank. For instance, let $B = 1$ and $K = \mathbb{Q}$. Interchanging x and y , we may write $E : y^2 - 2y = x^3$, which has conductor 36, and is curve 36a1 in Cremona's table [3, 10], and has rank 0 over \mathbb{Q} . On the other hand, one easily checks (e.g. using MAGMA) that E has rank 1 over $K = \mathbb{Q}(\sqrt{2})$, and $(1, 1 + \sqrt{2})$ is a non-torsion point in $E(K)$; it follows that $O_\phi(1 + \sqrt{2})$ has infinitely many distinct cubes in K . Note too that if we conjugate ϕ by the scaling $x \mapsto 3x$, we obtain the map given in (10.4) with $B = 3$. Now E is given by $y^2 - 6y = x^3$ (a twist of the previous E), which is curve 972c1 in Cremona's table, and has rank 1 over \mathbb{Q} . One finds that $(6, 18)$ is a generator for the free part of $E(\mathbb{Q})$, and thus $O_\phi(18)$ contains infinitely many distinct cubes – indeed, every element of $O_\phi(18)$ is a cube save for 18 itself.

10.5. Lattès maps of signature (2,2,2,2). It is here we obtain by far the most diverse behavior. We have $n = 2$ ([11, Remark 4.6]), which furnishes no restriction on Λ . Write $\Lambda = \mathbb{Z} + \gamma\mathbb{Z}$, and note that every orbit of the action of G_2 on \mathbb{C}/Λ has two elements, with the exception of

$$V_\Theta = \{[0], [1/2], [\gamma/2], [1/2 + \gamma/2]\},$$

where $[t]$ denotes the orbit of $t \in \mathbb{C}/\Lambda$ under $G_2 = \langle -1 \rangle$. We also use the notation V_Θ to refer to the subset $\{0, 1/2, \gamma/2, 1/2 + \gamma/2\}$ of \mathbb{C}/Λ . The action of ϕ on its post-critical set is then identical to the action of L on V_Θ . Note that the stipulation $(1 - \zeta_2)b \in \Lambda$ is the same as $2b \in \Lambda$, so that b is equivalent to an element of V_Θ modulo Λ . It is well-known that either $a \in \mathbb{Z}$ or a is an integer in an imaginary quadratic number field (see for instance [11, Lemma 5.4]). Note also that V_Θ is a subgroup of \mathbb{C}/Λ , and the map $t \mapsto at$ gives a homomorphism $a : V_\Theta \rightarrow V_\Theta$. Suppose that a is the zero-map and write $a = a_1 + a_2\gamma$ with $a_1, a_2 \in \mathbb{Z}$. Then $a \cdot 1/2 \in \Lambda$, which implies that a_1 and a_2

are even. Hence the map $L(t) = at + b$ maps V_Θ to itself four-to-one if and only if $a \equiv 0 \pmod{2\Lambda}$; otherwise the map is either one-to-one or two-to-one. The map ϕ has four 2-branch abundant points, namely those in V_Θ ; throughout this section, we let $A \subset V_\Theta$ have two elements.

Let us first examine the case when $a \equiv 0$ or $1 \pmod{2\Lambda}$, which must hold if \mathbb{C}/Λ does not have complex multiplication, for then $a \in \mathbb{Z}$. If $a \equiv 0 \pmod{2\Lambda}$, then L sends every element of V_Θ to b , which is a fixed point. Thus ϕ either has μ -type (12) (if $[b] \in A$) or (6,6). If $a \equiv 1 \pmod{2\Lambda}$ and $b \equiv 0 \pmod{\Lambda}$, then ϕ fixes each element of V_Θ , and hence has μ -type (1,1). If $a \equiv 1 \pmod{2\Lambda}$ and $b \not\equiv 0 \pmod{\Lambda}$, then L acts on V_Θ as two disjoint two-cycles. If the elements of A lie in a single two-cycle, then ϕ has μ -type (2) while otherwise ϕ has μ -type (2,2). This analysis shows that if ϕ is a flexible Lattès map and the genus of C_n is bounded, then ϕ is either trivial with respect to $\{0, \infty\}$ or has μ -type (12) or (2,2).

Suppose now that $a \not\equiv 0$ or $1 \pmod{2\Lambda}$, which implies $a \notin \mathbb{Z}$, and hence a satisfies an equation of the form

$$a^2 = c_2 a + c_1 \quad \text{with} \quad c_2, c_1 \in \mathbb{Z}.$$

Note that $t \mapsto (a+1)t$ induces a homomorphism $(a+1) : V_\Theta \rightarrow V_\Theta$, and thus the number of fixed points of the action of $L(t) = at + b$ on V_Θ is either $\#\ker(a+1)$ (if $b \in \text{im}(a+1)$) or zero, since $a-1 \equiv a+1 \pmod{2\Lambda}$. We claim that

$$\#\ker(a) = \begin{cases} 1 & \text{if } c_1 \equiv 1 \pmod{2} \\ 2 & \text{if } c_1 \equiv 0 \pmod{2} \end{cases} \quad \text{and} \quad \#\ker(a+1) = \begin{cases} 1 & \text{if } c_1 \equiv c_2 \pmod{2} \\ 2 & \text{if } c_1 \not\equiv c_2 \pmod{2} \end{cases}$$

To see why, suppose that $c_1 \equiv 1 \pmod{2}$. Then $a(a+c_2) \equiv 1 \pmod{2\Lambda}$, and thus $av \equiv 0 \pmod{\Lambda}$ for $v \in V_\Theta$ implies $v \equiv (a+c_2)0 \equiv 0 \pmod{\Lambda}$. If $c_1 \equiv 0 \pmod{2}$, then $a(a+c_2) \equiv 0 \pmod{2\Lambda}$, which implies that the image of the homomorphism $(a+c_2) : V_\Theta \rightarrow V_\Theta$ is contained in $\ker(a)$. But $(a+c_2)$ cannot be the zero map, because $a \not\equiv 0$ or $1 \pmod{2\Lambda}$, and thus $\#\ker(a) \geq 2$. But a is also not the zero map, and hence $\#\ker(a) = 2$. The statement for $\ker(a+1)$ follows from the same reasoning and the fact that $(a+1)^2 \equiv (c_1+c_2+1) + c_2(a+1) \pmod{2\Lambda}$.

Suppose that $c_1 \equiv c_2 \equiv 1 \pmod{2}$. Then $L(t) = at + b$ acts on the four-element set V_Θ one-to-one and with a unique fixed point, and hence the action consists of a fixed point and a 3-cycle. Therefore ϕ has μ -type (3,1) if A contains the fixed point, and μ -type (3) otherwise.

If $c_1 \equiv c_2 \equiv 0 \pmod{2}$, then L acts on V_Θ two-to-one with a unique fixed point. A 2-cycle of a two-to-one map requires four points, and thus L has no 2-cycle, and hence sends two non-fixed points to a third, which then maps to the unique fixed point. Therefore ϕ has μ -type (6,6), (8), (10a), or (10b), depending on the locations of the points of A in V_Θ .

If $c_1 \equiv 1 \pmod{2}$ and $c_2 \equiv 0 \pmod{2}$, then L acts on V_Θ one-to-one with either two fixed points (if $b \in \text{im}(a+1)$) or no fixed points. In the former case, the action must consist of two fixed points and a 2-cycle, and thus ϕ has μ -type (1,1), (2), or (2,1), depending on the locations of the points of A . In the latter case, L must act on V_Θ as either a single 4-cycle or two 2-cycles. We claim that because $b \notin \text{im}(a+1)$, the action cannot have a 2-cycle and thus must consist of a single 4-cycle, and so ϕ has μ -type (5a) or (5b). Indeed, $(a+1)^2 \equiv 0 \pmod{2\Lambda}$, and so $\text{im}(a+1) \subseteq \ker(a+1)$. But $\#\text{im}(a+1) = \#\ker(a+1) = 2$, and so $\text{im}(a+1) = \ker(a+1)$. Thus if $b \notin \text{im}(a+1)$ then also $b \notin \ker(a+1)$, and so for any $v \in V_\Theta$ we have $L(L(v)) = a^2 v + b(a+1) \equiv v + b(a+1) \not\equiv v \pmod{2\Lambda}$. Hence v does not lie in a two-cycle.

If $c_1 \equiv 0 \pmod{2}$ and $c_2 \equiv 1 \pmod{2}$, then L acts on V_Θ two-to-one with either two fixed points (if $b \in \text{im}(a+1)$) or no fixed points. In the former case, the action must consist of two fixed points, each mapped to by one non-fixed point. Hence ϕ has μ -type (6,6), (7), (7,6), or (7,7), depending on the locations of the points of A . In the latter case, L must have a 2-cycle, for a 3-cycle of a two-to-one

mapping requires six points. Each point in this 2-cycle is mapped to by a single point not in the 2-cycle, and so ϕ has μ -type (6,6), (11a), (11b), or (11c).

10.6. Field of definition and field of moduli. We now examine the question of whether maps of certain μ -types may be defined over a given field. Let K be a number field with $\phi \in K(x)$, and recall from [13] that a number field L is a *field of definition* for ϕ if there exists a Möbius transformation $\nu \in \mathrm{PGL}_2(\mathbb{C})$ such that $\nu \circ \phi \circ \nu^{-1} \in L(x)$. The *field of moduli* of ϕ is the fixed field of

$$G_\phi := \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \text{there exists } \nu \in \mathrm{PGL}_2(\mathbb{C}) \text{ with } \phi^\sigma = \nu \circ \phi \circ \nu^{-1}\},$$

where ϕ^σ denotes the map obtained by letting σ act on the coefficients of ϕ . We remark that for $P \in \overline{K}$ we have $\phi^\sigma(P) = \sigma \circ \phi \circ \sigma^{-1}(P)$. If $\nu \circ \phi \circ \nu^{-1} \in L(x)$ then clearly $(\nu \circ \phi \circ \nu^{-1})^\sigma = \nu \circ \phi \circ \nu^{-1}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$. It follows that $\phi^\sigma = \nu_1 \circ \phi \circ \nu_1^{-1}$, where $\nu_1 = (\nu^\sigma)^{-1} \circ \nu$. Hence if L is a field of definition for ϕ then $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \leq G_\phi$, and therefore L contains the field of moduli for ϕ .

Proposition 10.1. *Let K be a number field and $\phi \in K(x)$ a Lattès map of signature (2,2,2,2) and degree at least two, descending from $L(t) = at + b$. Suppose that $a \notin \mathbb{Z}$ and $a^2 = c_2a + c_1$ with $c_2, c_1 \in \mathbb{Z}$ and $c_2 \neq 0$. Then a is contained in the field of moduli for ϕ . Thus a lies in any field of definition for ϕ , and in particular $a \in K$.*

Proof. We must show that for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\sigma(a) \neq a$, the maps ϕ and ϕ^σ are not conjugate by a Möbius transformation. Denote by $\mathrm{FixSpec}(\phi)$ the set of multipliers of all fixed points of ϕ , and recall that this set is invariant under replacing ϕ by a Möbius conjugate. From [11, Corollary 3.9] we have $\mathrm{FixSpec}(\phi) \subseteq \{\pm a, a^2\}$. One easily sees that $\mathrm{FixSpec}(\phi^\sigma) = \sigma(\mathrm{FixSpec}(\phi))$, and so it suffices to show that $\sigma(\{\pm a, a^2\}) \cap \{\pm a, a^2\} = \emptyset$. Because $a \notin \mathbb{Z}$, the minimal polynomial of a over \mathbb{Q} must be $x^2 - c_2x - c_1$, and the quadratic formula gives that the set of Galois conjugates of a is $\{a, -a + c_2\}$. By assumption $\sigma(a) \neq a$, and if $\sigma(a) = -a$ then $-a + c_2 = -a$, contradicting $c_2 \neq 0$. If $\sigma(a) = a^2$ then $-a + c_2 = c_2a + c_1$, and so $c_2 = -1$ and $c_1 = c_2 = -1$, whence a has norm 1 and so ϕ has degree 1, contrary to assumption. This establishes that $\sigma(\{\pm a\}) \cap \{\pm a, a^2\} = \emptyset$. If $\sigma(a^2) = a^2$, then $c_2\sigma(a) + c_1 = c_2a + c_1$, and because $c_2 \neq 0$ it follows that $\sigma(a) = a$, a contradiction. If $\sigma(a^2) = \pm a$, then $a^2 = \pm\sigma(a)$, and so $c_2a + c_1 = \pm(-a + c_2)$, whence $c_2 = \pm 1$ and $c_1 = \pm c_2 = \mp 1$. It follows that ϕ has degree 1, again contrary to supposition. \square

Corollary 10.2. *Let K be a number field and $0, \infty$ be 2-branch abundant points for $\phi \in K(x)$. If ϕ has μ -type (3,1), (11a), (11b), or (11c), then $K \not\subset \mathbb{R}$. In particular, $K \neq \mathbb{Q}$.*

Remark. Milnor arrives at a similar result for a Lattès map of signature (3,3,3), using a different argument [11, p. 27, Section 8.2].

Proof. From Table 2 any map of μ -type (3,1), (11a), (11b), or (11c) must be Lattès of signature (2,2,2,2). From the analysis on p. 45, any Lattès map with one of these μ -types must satisfy $c_2 \equiv 1 \pmod{2}$. The Corollary now follows from Proposition 10.1 and the observation that $a \notin \mathbb{R}$. \square

Corollary 10.3. *Let K be a number field and A a set of two distinct 2-branch abundant points for $\phi \in K(x)$. If ϕ has μ -type (3,1), then the multiplier of the post-critical fixed point of ϕ is a square in K .*

Proof. From [11, Corollary 3.9] the multiplier of the post-critical fixed point is a^2 . From Proposition 10.1 we have $a \in K$, proving the Corollary. \square

Now suppose that $\phi \in K(x)$ is a Lattès map of signature (2,2,2,2) with $a \notin \mathbb{Z}$ and $c_2 = 0$. Then the argument used to prove Theorem 10.1 fails, and indeed one has $\mathrm{FixSpec}(\phi) = \mathrm{FixSpec}(\phi^\sigma)$ for

all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It seems plausible that in fact ϕ and ϕ^σ are always Möbius conjugate, or in other words the field of moduli of ϕ is \mathbb{Q} . If so, this raises the question of whether \mathbb{Q} is a field of definition for ϕ . It is shown in [13] that the field of moduli is not always a field of definition (for maps of odd degree), and it would be interesting to have Lattès maps that provide examples of this.

From our previous analysis, there exist Lattès maps with a post-critical four-cycle and $c_2 = 0$. This raises the following questions:

Question 10.4. *Can a Lattès map with a post-critical four-cycle be defined over \mathbb{Q} ? Can a Lattès map with a post-critical four-cycle containing 0 and ∞ be defined over \mathbb{Q} ?*

If the answer to the second question is negative, then for $K = \mathbb{Q}$ the quantity M from Theorem 1.1 is at most $\max\{3, m\}$. We give below an example of a map of μ -type (5a) defined over $\mathbb{Q}(\sqrt{3})$ that shows $m = 2, M = 4$ is possible over general number fields, and in Section 10.7 we give an example to show $m = 2, M = 3$ is possible over \mathbb{Q} .

We now construct an example of a rational function of degree 3 with $c_2 = 0$ and μ -type (5a) for $A = \{0, \infty\}$. These conditions imply that $a = \pm\sqrt{-3}$ and $\Lambda = \mathbb{Z}[\sqrt{-3}]$, for if $\Lambda = \mathbb{Z}[(1 + \sqrt{-3})/2]$ then $a \equiv 1 \pmod{2\Lambda}$, which precludes μ -type (5a) or (5b). We begin with the map

$$(10.5) \quad \phi(x) = \frac{x(x - (2s - s^2))^2}{(x - 1)(x - s^2)^2},$$

which has been chosen so that $0, 1, \infty$ are critical values but not critical points, 0 is a fixed point, and 1 and ∞ are in a 2-cycle. The fourth critical point of ϕ is given by $\gamma := \frac{2s-s^2}{2s-1}$, and we wish to select s so that $\phi(\gamma)$ is a fixed point that is not equal to γ . We calculate the numerators of $\phi^2(\gamma) - \phi(\gamma)$ and $\phi(\gamma) - \gamma$, and find that taking $s = -1 \pm \sqrt{3}$ makes the former zero but not the latter. When s has this value, (10.5) is a Lattès map, which descends from $L(t) = \pm\sqrt{-3}$. Moreover, its fourth critical value is the fixed point $\phi(\gamma) = -4s + 4$. To construct a map of signature (5a) or (5b), we require ϕ to have a post-critical four-cycle. This can be done by post-composing ϕ with a Möbius transformation that interchanges 0 and ∞ and also interchanges 1 and $-4s + 4$. Taking $h(x) = (-4s + 4)/x$ suffices, and the map

$$(10.6) \quad \phi_1(x) := h(\phi(x)) = (-4s + 4) \frac{(x - 1)(x - (2 - 2s))^2}{x(x - (4s - 2))^2} \quad s = -1 \pm \sqrt{3}$$

has the four-cycle $0 \mapsto \infty \mapsto -4s + 4 \mapsto 1 \mapsto 0$, each of which is a critical value. This map has μ -type (5a). If we take $x = 4$, one can check using the data from Table 4 that $\phi_1^{4n+i}(4) \notin K^2$ for $i \in \{1, 2, 3\}$ and all $n \geq 0$. Because $\phi_1^4(x) \equiv x \pmod{K(x)^{*2}}$, it follows that $O_{\phi_1}(4) \cap \mathbb{P}^1(K)^2 = \{\phi_1^{4n}(4) : n \geq 0\}$. Moreover, $O_{\phi_1}(4)$ is infinite. We close this subsection with a special case of Question 10.4:

Question 10.5. *Is the map in (10.6) Möbius-conjugate to a map defined over \mathbb{Q} ? Is the map in (10.6) Möbius-conjugate to a map defined over \mathbb{Q} that also has 0 and ∞ in the post-critical four-cycle?*

10.7. Non-Lattès examples for $m = 2$. As seen in Section 10.5, one may find examples of Lattès maps with μ -types (2,1), (3), (7,6), and (8). However, non-Lattès examples are much more plentiful, and are straightforward to construct.

We first give an example of a map of μ -type (3), which must have form in (5a) of Theorem 1.3. Set $f(x) = x - r$ and $g(x) = x - s$, and note that taking $x = 0$ in the equation $f(x)^2 + C(x - C)g(x)^2 = Cxh(x)^2$ implies $r^2 - C^2s^2 = 0$, and so $r = \pm Cs$. We take $r = Cs$ and then find the discriminant of $(f(x)^2 + C(x - C)g(x)^2)/Cx$ to be $\pm(C - 1)^2(C^2 + 2C + 1 - 4Cs)$. Because $C \neq 1$ (otherwise $r = s$,

and so the numerator and denominator of ϕ have a common root), we must have $s = (C + 1)^2/4C$. Multiplying numerator and denominator by $(4C)^2$ yields the family of maps

$$(10.7) \quad \phi(x) = -C^2 \frac{(4x - (C + 1)^2)^2}{(x - C)(4Cx - (C + 1)^2)^2},$$

where we require $C \notin \{-1, -1/3, 0, 1\}$ in order to meet the conditions of part (5a) of Theorem 1.3. Note that ϕ has μ -type (3) and the post-critical three-cycle $\infty \mapsto 0 \mapsto C \mapsto \infty$. Three of the critical points of ϕ map to 0, C , and ∞ , respectively. The fourth critical point $\gamma = (3c^2 + 2c - 1)/4$ is not in general pre-periodic, and hence ϕ is not in general post-critically finite, in contrast to Lattès maps.

Taking $C = 3$ in (10.7) gives the map

$$\phi(x) = -\frac{9(x - 4)^2}{(x - 3)(3x - 4)^2},$$

One can check that the critical point $\gamma = 8$ is not pre-periodic, and hence ϕ is not post-critically finite. The orbit of 1 under ϕ is infinite, and we have

$$O_\phi(1) = \left\{ 1, 2 \left(\frac{9}{2} \right)^2, -6 \left(\frac{73}{1175} \right)^2, \left(\frac{3263253475}{1913072691} \right)^2, \dots \right\}.$$

Indeed, the squares in $O_\phi(1)$ consist of the set $\{\phi^{3k}(1) : k \geq 0\}$. It follows from the data in Table 4 that $\phi^{3k+1}(1)$ is twice a square for all $k \geq 0$, and $\phi^{3k+2}(1)$ is -6 times a square for all $k \geq 0$. We may also take $C = 2$ in (10.7), and then find that $\{n \geq 0 : \phi^n(4) \in \mathbb{P}^1(\mathbb{Q})^2\}$ consists of the union of the two infinite arithmetic progressions $\{3k : k \geq 0\}$ and $\{3k + 2 : k \geq 0\}$.

We now study examples of μ -type (7,6), which have particular interest by the last paragraph of the proof of Theorem 1.1: only maps of this μ -type may have an orbit with infinitely many squares, and where the index set of the squares can be written as a disjoint union of three arithmetic progressions, but not two. We now show that this phenomenon occurs even for $K = \mathbb{Q}$. Examples of μ -type (7,6) must have form in (5d) of Theorem 1.3. Set $f(x) = 1$ and $g(x) = x - s$, and note that this gives (up to conjugation by $x \mapsto 1/x$ the unique degree-2 family of maps of μ -type (7,6), since one may pull constant factors out of $f(x)^2$ and $g(x)^2$ and absorb them into B ; doing so only changes B by a square, which does not affect our analysis.

Now the discriminant of $(Bx(x - C) - C(x - s)^2)/(-C)$ is $BC(BC - 4Cs + 4s^2)$, and to make this discriminant zero we take $B = 4s(c - s)/c$. We wish for s to have a rational preimage under ϕ , and so we find that the discriminant of the numerator of $\phi(x) - s$ is $16s^2(C - s)^3/C$. We wish for this to be a square, and hence we take $(C - s)/C = d^2$, i.e. $s = C(1 - d^2)$. Doing so gives

$$\phi^{-1}(s) = \left\{ \frac{C(d + 1)^2}{2d + 1}, -\frac{C(d - 1)^2}{2d - 1} \right\}.$$

Letting $v = C(d + 1)^2/(2d + 1)$, we have the orbit

$$(10.8) \quad v \mapsto s \mapsto \infty \mapsto B \mapsto \phi(B) \mapsto \dots$$

From Table 4, we have $\phi(x) \equiv Bx(x - C)$ and $\phi^2(x) \equiv -Cx(x - C)$ modulo $K(x)^{*2}$, and also $\phi^n(x) \equiv \phi^n - 2(x) \pmod{K(x)^{*2}}$ for all $n \geq 3$. We wish for the squares in (10.8) to appear at indices $\{0, 2\} \cup \{2n + 1 : n \geq 0\}$, which cannot be written as a union of fewer than three arithmetic progressions. We thus require both v and s to be squares in K , and to ensure $\{\phi^{2n+1}(v) : n \geq 0\}$ consists of squares and $\{\phi^{2n+2}(v) : n \geq 1\}$ consists of non-squares, we need for $-C\phi(v)(\phi(v) - C)$ to be a square in K and $\phi^4(v)$ to be a non-square in K . This last condition is the same as $\phi(B)$

being a non-square in K , and because $\phi^{2n+1}(B) \equiv \phi(B) \pmod{K^{*2}}$ this shows that $\{\phi^{2n+2}(v) : n \geq 1\}$ consists of non-squares. We have

$$v \equiv C(2d+1) \pmod{K^{*2}} \quad s \equiv C(1-d^2) \pmod{K^{*2}}$$

$$-C\phi(v)(\phi(v)-C) = -Cs(s-C) \equiv -C(C(1-d^2))(C(1-d^2)-C) \equiv C(1-d^2) \pmod{K^{*2}}$$

$$\phi^4(v) = \phi(B) = -16Cd^4(2d^2-1)^2/(4d^2-1)^2 \equiv -C \pmod{K^{*2}}$$

Thus we wish to have $C(2d+1) \in K^{*2}$, $C(1-d^2) \in K^{*2}$, and $-C \notin K^{*2}$. If d satisfies these conditions, then it gives rise to a K -rational point on the elliptic curve

$$E : y^2 = (2d+1)(1-d^2).$$

This curve has conductor 24, and is isomorphic to curve 24a1 in Cremona's table [3]. It has rank zero over \mathbb{Q} and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/4\mathbb{Z}$. Among the seven finite torsion points are three with $y = 0$ and two with $d = 0$, which force one of $v = 0$, $s = 0$, or $s = C$, and thus cannot hold in our setting. The other two points are $(d, y) = (-2, \pm 3)$, and so $d = -2$ is the only possibility over \mathbb{Q} . With this choice, we may take $C = -3t^2$ for any $t \in \mathbb{Q} \setminus \{0\}$ to satisfy our conditions. This gives rise to the family

$$(10.9) \quad \phi(x) = \frac{144t^2x(x+3t^2)}{(x-9t^2)^2} \quad t \in \mathbb{Q} \setminus \{0\},$$

which is the unique family over \mathbb{Q} satisfying our conditions. The orbit

$$O_\phi(t^2) = \left\{ t^2, 9t^2, \infty, 144t^2, 3\left(\frac{112t}{5}\right)^2, \left(\frac{151872t}{11869}\right)^2, 3\left(\frac{17917453568t}{807305405}\right)^2, \dots \right\}$$

has squares occurring at index set $\{0, 2\} \cup \{2n+1 : n \geq 0\}$, as desired.

Question 10.6. *Aside from the family in (10.9), are there rational functions with coefficients in \mathbb{Q} possessing an orbit with infinitely many squares, such that the index set of the squares cannot be written as a union of two arithmetic progressions?*

We close with an example of a two-parameter family of maps of μ -type (8), obtained by taking $f(x) = 1$ and $g(x) = x - s$ in (5c) of Theorem 1.1:

$$\phi(x) = 4C(C-s)\frac{(x-C)}{(x-s)^2}, \quad C, s \in K, C \neq 0, s \neq C$$

These maps have the extraordinary property that $\phi(x) \notin \mathbb{C}(x)^{*2}$ but $\phi^2(x) \in \mathbb{C}(x)^{*2}$, as noted in Corollary 1.10. Indeed, from Table 4 one sees that taking $-BC \in K^2$, i.e. $(s-C) \in K^2$, we have $\phi^2(x) \in K(x)^{*2}$.

ACKNOWLEDGEMENTS

We thank Tommy Occhipinti, Bjorn Poonen, Joe Silverman, and Tom Tucker for helpful comments.

REFERENCES

- [1] Alan F. Beardon. *Iteration of rational functions*, volume 132 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Complex analytic dynamical systems.
- [2] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. The dynamical Mordell-Lang conjecture. Book manuscript. Preprint, 2015.
- [3] John Cremona. The elliptic curve database for conductors to 130000. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 11–29. Springer, Berlin, 2006.
- [4] D. Ghioca and T. J. Tucker. Periodic points, linearizing maps, and the dynamical Mordell-Lang problem. *J. Number Theory*, 129(6):1392–1403, 2009.
- [5] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve. Intersections of polynomials orbits, and a dynamical Mordell-Lang conjecture. *Invent. Math.*, 171(2):463–483, 2008.
- [6] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve. Linear relations between polynomial orbits. *Duke Math. J.*, 161(7):1379–1410, 2012.
- [7] Chad Gratton, Khoa Nguyen, and Thomas J. Tucker. ABC implies primitive prime divisors in arithmetic dynamic. To appear, *Bull. Lond. Math. Soc.* Available at <http://arxiv.org/abs/1208.2989>.
- [8] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.
- [9] Gregory Karpilovsky. *Topics in field theory*, volume 155 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1989. Notas de Matemática [Mathematical Notes], 124.
- [10] The LMFDB Collaboration. The l-functions and modular forms database. <http://www.lmfdb.org>, 2013. [Online; accessed 16 September 2013].
- [11] John Milnor. On Lattès maps. In *Dynamics on the Riemann sphere*, pages 9–43. Eur. Math. Soc., Zürich, 2006.
- [12] Joseph H. Silverman. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.*, 71(3):793–829, 1993.
- [13] Joseph H. Silverman. The field of definition for dynamical systems on \mathbf{P}^1 . *Compositio Math.*, 98(3):269–304, 1995.
- [14] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [15] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.